DATA REVELATIONS

Nominum Data Science Security Report

nominum™

Spring 2017

EXECUTIVE SUMMARY

Since our **Fall 2016 Data Revelations Report**, the world has been abuzz with talk of cybercrime. No longer confined to cybersecurity blogs or industry conferences, 2016 was the year cybersecurity dominated the headlines.

Consider the Dyn attacks in October where Twitter, Netflix, the New York Times and other trusted websites went offline for hours. Or the ransomware attack that took San Francisco's Municipal Railway (MUNI) ticketing system offline in November. Or the April 2017 arrest of a well-known cybercrime kingpin who is allegedly responsible for the well-known Kelihos botnet and may have been involved with the hacking of the Democratic National Committee.

In 2017, Nominum Data Science has witnessed significant increases in cybercrime. As the DNS supplier to service providers serving over one-third of the world's internet subscribers, Nominum has a unique vantage point from which to investigate internet security threats. By analyzing over 100 billion DNS queries every day from around the world, Nominum uncovers patterns and anomalies to inform real-time threat intelligence feeds that keep our customers' networks, businesses and consumers safe.

The good news is that cybercrime is not a black box: it is an efficient, rational market, which can be analyzed like any other market; it has products, services and processes, albeit malicious ones, which can be examined and evaluated. Once an attacker's motivations and tactics are understood, it is easier to prescribe and develop the right countermeasures. In this report, we introduce the Nominum Cyberattack Ladder, a framework that looks at cybercrime from a criminal's perspective and breaks down the various processes and stages of an attack.

This report will include findings from a six-month period, which include:

- **Malware query increases:** Why we see a 404 percent increase in the average number of malicious queries per day.
- **Phishing expands:** We examine the current state of phishing, including what happens within five to 10 hours of a mobile phishing launch.
- **PRSD attacks intensify:** Attacks grew 68 percent in the first three months of the year. We discuss the botnet we think is responsible for this increase.
- **Ransomware escalates:** Ransomware queries grew 270 percent between Fall 2016 and Spring 2017. We share top threats and break down the lifecycle of an attack.
- **IoT threats rise:** Princeton Professor Nick Feamster shares his perspective on IoT and the role of DNS in detection.

Enjoy the report. If you have feedback or questions, please contact **hello@nominum.com**.

Warm regards,

Yohai Einav, Principal Security Researcher

Yuriy Yuzifovich, Head of Data Science & Security Research

CONTENTS

WELCOME TO THE CYBERATTACK LADDER

> "In research of all traditions, metaphor is used as a conceptual tool to make concrete, and make sense of, complex phenomena."
>
> **JOY L. EGBERT AND GINA MIKEL PETRIE, CALL RESEARCH PERSPECTIVES**

INTRODUCTION

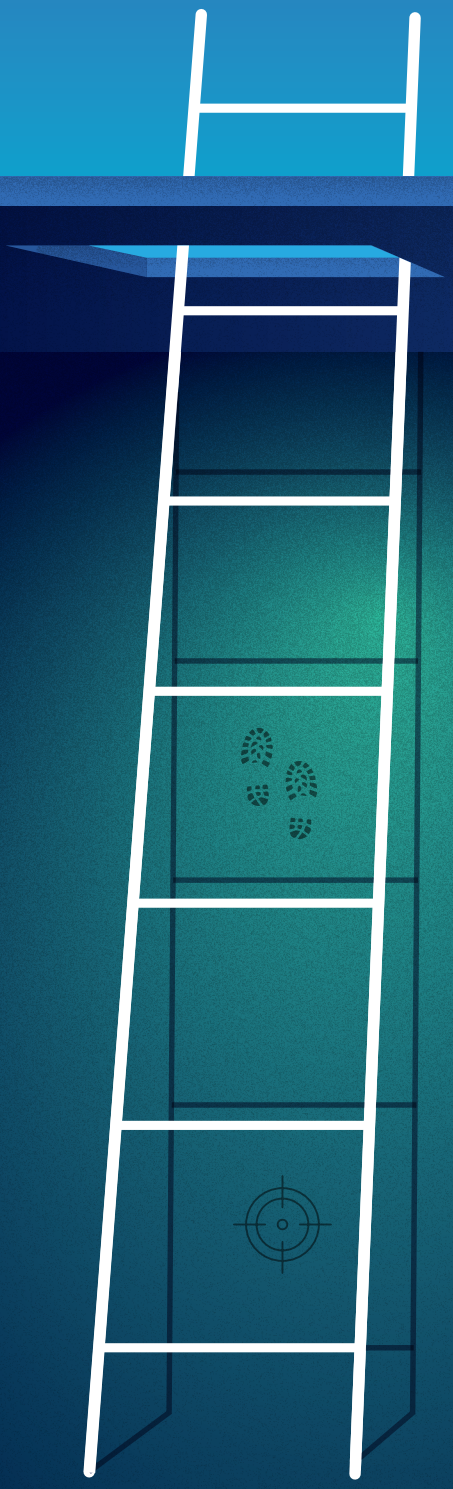
It is hard to avoid metaphors when discussing cybersecurity. It's a complex field that incorporates too many intangibles that are difficult to understand without grounding them in everyday experience.

A commonly used metaphor for cybersecurity is that of a fortress: a prized body of information (computer or network) is held within walls, encircled by a moat, accessed by portals or gates, and guarded by watchmen assigned to keep out the unauthorized. Given this theme, computer users are expected, for instance, to use firewalls to protect against Trojan Horses and put Kerberos, the three-headed hound of Hades, in charge of network authentication processes.

The term Cyber Kill Chain® is another well-known cybersecurity metaphor that was coined by defense giant Lockheed Martin to describe different stages of a cyberattack. The framework derives from a basic military model, originally established to identify, prepare for, engage and destroy the target. The idea here is to look at things from an attacker's perspective, rather than from the defender's point of view.

While the Kill Chain is a commonly used metaphor, we at Nominum believe that the process of cyberattack is a bottoms-up one. We therefore devised the Cyberattack Ladder, a framework where the foundational components of a cyberattack, such as preparation and intrusion, must be completed at the bottom rungs before a full-scale attack can occur at the top of the ladder. If initial steps of an attack are prevented, the cybercriminal's ultimate goal will not be realized. Thus, ransomware extortion or large-scale DDoS attacks cannot occur without phishing, botnets, C&C communications and a host of other steps.

THE NOMINUM CYBERATTACK LADDER



3: ATTACK STAGE

ACTION
Use compromised device to perform attacks (DDoS), manipulate data (ransomware), send spam and more

C&C
Establish remote communication with command server to receive commands, send data

2: INTRUSION STAGE

INSTALLATION
Install malware on target device

EXPLOITATION
Exploit vulnerability on target devices to execute malware code

DELIVERY
Deliver “weaponized” payload to victim’s device via email, web, text; typically using social engineering

1: PREPARATION STAGE

WEAPONIZATION
Acquire, exploit, write or buy malware, then associate them to create initial payload

RECONAISSANCE
Harvest email addresses of potential target and victims, gather information from social networks and other public sources

Steps in the Cyberattack Ladder can be categorized into three stages: the preparation stage, which includes reconnaissance and weaponization, an intrusion stage, which includes delivery, exploitation and installation, and finally, the attack stage, which includes C&Cs and action on objectives.

The Nominum Cyberattack Ladder helps organizations better understand the risks they face in each stage and consider whether they have the right protection mechanisms in place. Because over 90 percent of malware relies on DNS[1], it plays a crucial role in cyberthreat analysis and prevention. Without DNS, there would be no internet, online services or smart phone apps. As the "phone book" of the internet, DNS translates a name (e.g., www.nominum.com) to an IP address. DNS offers a unique vantage point because cybercriminals use it regularly. From cache poisoning, where cybercriminals insert corrupt data into the DNS cache, to Trojans that alter DNS settings to DNS hijacking, there are a variety of ways cybercriminals exploit DNS for malicious purposes.

This report will describe the different, relevant points where DNS plays a crucial role in threat prevention. We use the ladder to examine ransomware as it evolves from the preparation stage, where relevant information about the target is gathered, to the intrusion stage, where phishing emails or spam are used to deliver the malicious payload, and, finally, to the attack stage, where it takes over a device and its data, communicates with its C&C, and where the attacker tries to extort ransom money from the victim.

Why DNS Goes Beyond the Phone Book Metaphor

DNS does map (domain) names to (IP) numbers in the same way that a phone book matches a name with a number but this misses some important elements of the technology. If DNS is a phone book, then it's a phone book where you can see who calls whom, when, from where, using what type of phone, who answers the call on the other end, when and where it was answered and in what language. Furthermore, you can get that information for any call, anywhere in the world. No phone book, even in 2017, can do all that.

When you have access to voluminous DNS information, including the 100 billion anonymized DNS queries we at Nominum analyze daily, you can utilize it for doing good, like providing stronger security to internet users. All you need is this great source of mobile, fixed and geographically-diverse data combined with a group of skilled and creative data scientists and engineers.

[1] http://blogs.cisco.com/security/overcoming-the-dns-blind-spot

ANALYSIS TIMEFRAME:
SEP 2016 – FEB 2017

TOTAL QUERY VOLUME:
15.3 TRILLION

AVERAGE UNIQUE DOMAINS/DAY:
533.7 MILLION

Methodology

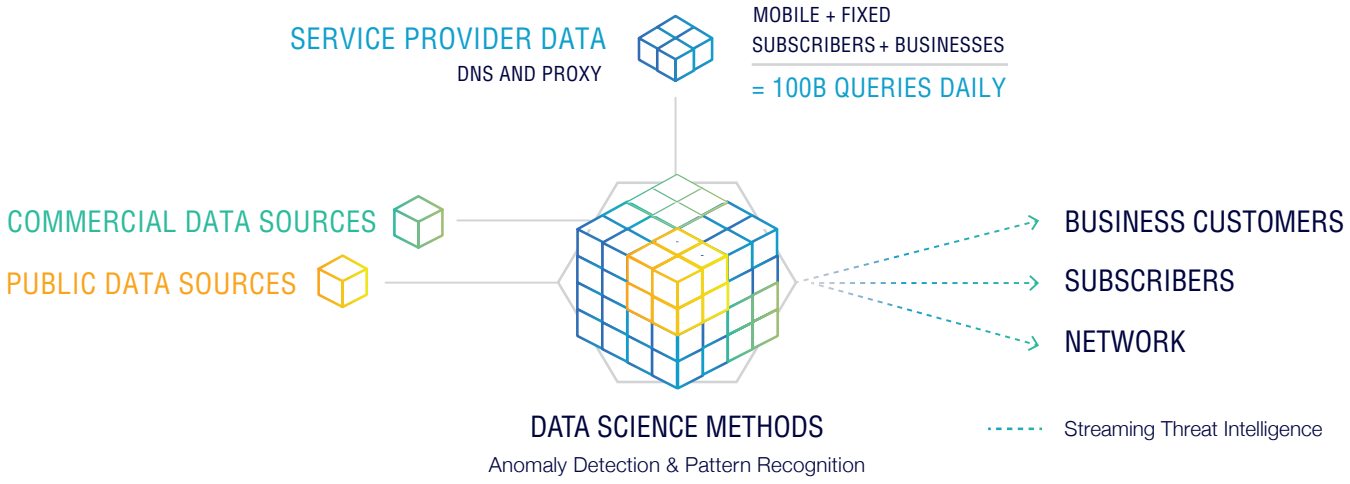
To offer proactive protection, Nominum Data Science analyzes daily, weekly and quarterly data sets to predict the next steps cybercriminals will take. The goal: detect attack signals in the sea of DNS data, and validate known attack types while simultaneously detecting new, unknown and unnamed malicious activity.

DNS and DNS data are the lifeblood of the internet. Data and data analyses are the essence of Nominum Data Science and our cybersecurity work. This report is a culmination of several months of analysis as detailed below. This sample represents approximately three percent of total global traffic, generated by consumers and businesses.

Tools, Inputs and Outputs

Nominum Data Science detects threats using DNS data. In addition to using commercial and public data sources, the team analyzes 100 billion queries daily from Nominum customers. As background, Nominum works with more than 130 service providers in over 40 countries, resolving 1.7 trillion queries daily.

A variety of proprietary data analytics tools and algorithms are used for pattern recognition and anomaly detection.



- **Domain Reputation System (DRS):** A large-scale, comprehensive, knowledge-based system for domain names and their related entities. This tool detects subtle links between domains, hosting servers, name servers, WHOIS information and blacklist data, and measures the maliciousness of each domain based on its relationships.
- **Anomaly Detection Engine:** Identifies anomalies in the data by comparing each queried domain to previous domain behaviors, or by identifying newly-generated domains.
- **Correlation Engine:** Identifies subtle relationships between domain names and the clients that query them. This tool uses machine learning to detect and cluster families of malicious domains.

Threat intelligence is streamed to Nominum customers to protect their internal infrastructure, subscribers and business customers. We like to think of the process as "closed loop" streaming, in that we feed intelligence to customers and their data, in turn, is streamed to us for threat detection. This virtuous cycle keeps fresh data "in the pipe" for analysis by Nominum detection systems while ensuring that fast-moving threats detected in one provider's data is quickly blocked for all other customers.

In this report, we introduce a new analytics tool, the Nominum Zero-day Quarantine Engine. This tool uses machine learning algorithms to isolate and cluster domains that have not been seen before, and then quarantines the domains that have a high probability of being malicious. More details about this tool and its process will be provided later in this report.

Threat Tracker

We introduced the Nominum Threat Tracker in the **Fall 2016 Data Revelations Report**. The tracker looks into activities, trends and relationships among malicious domains, infected clients, and the queries generated by the infected clients. It provides a big-picture view and helps identify where the main threats lurk and where the next innovation is needed, all grounded in actual (big) data.

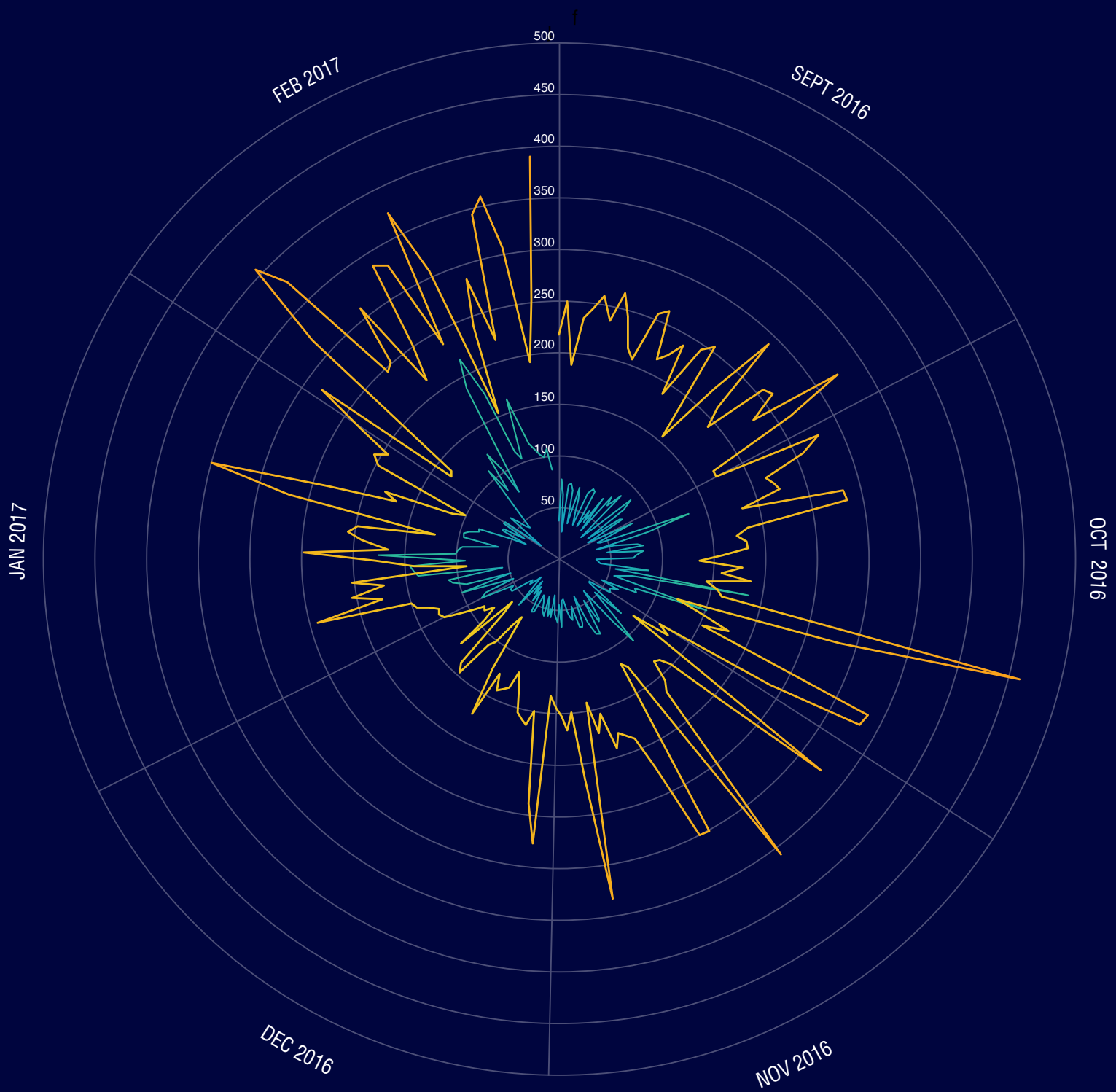
After a "slow" end of year, the number of malicious queries jumped in January and February 2017 to an all-time high. The average number of malicious queries per day from September through December 2016 was 59 million, while in January and February 2017, the number crossed the 91 million mark (over 50 percent growth). The median number of queries per day in February 2017 was over 100 million and reached a single-day, all-time high of 216.6 million queries on February 17.

After reviewing data for the six-month period (September through February), we took a broader view and examined data dating back to March 2016. (The Fall 2016 edition of Nominum Data Revelations looked at data from March through August 2016). We witnessed, through fine-tuned detection methods, substantial growth: from a median of 19 million malicious queries per day in March 2016 to 101 million in February 2017, or 404 percent average daily growth over the year, as seen in **Chart 1**.

After a "slow" end of year, the number of malicious queries jumped in January and February 2017 to an all-time high.

THREAT TRACKER SPRING 2017

Queries (in Millions) **Domains** (in Thousands)



HIGHEST MALICIOUS QUERIES IN A SINGLE DAY

217 M

GROWTH IN AVERAGE MONTHLY MALICIOUS QUERIES

47%

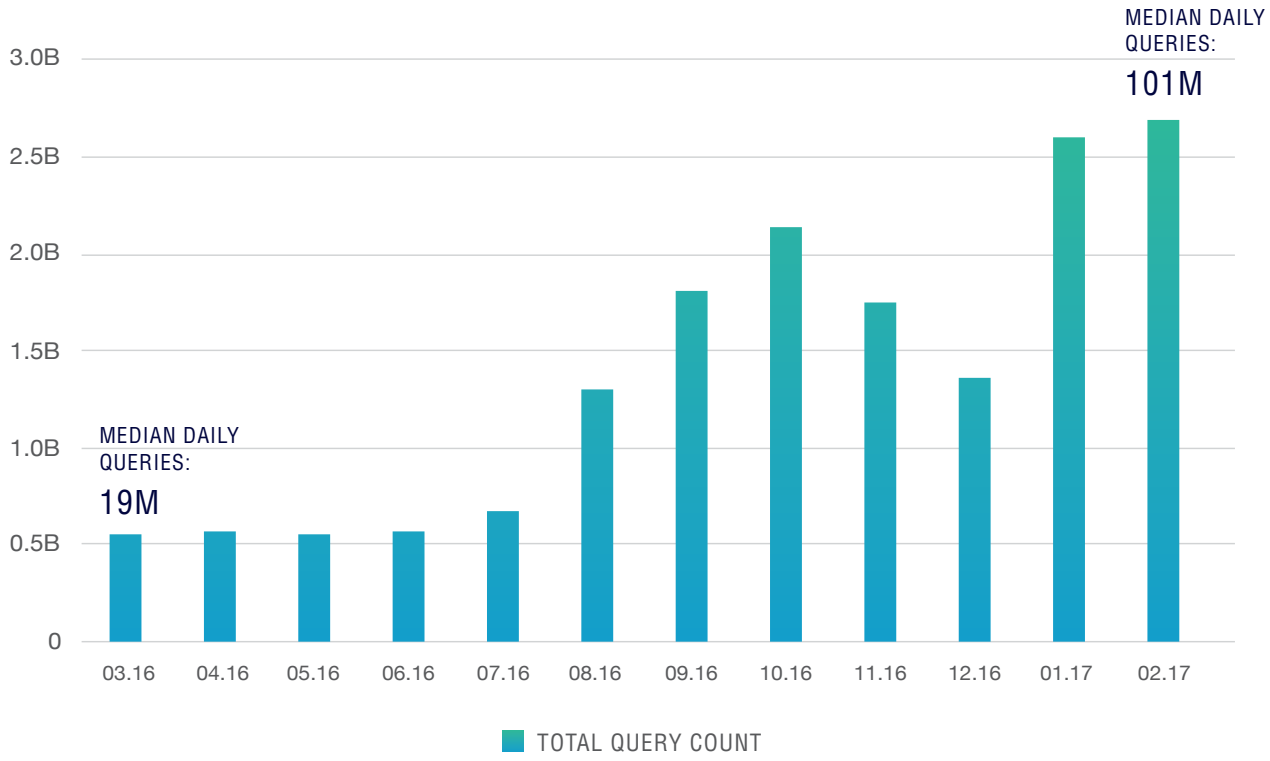
GROWTH IN AVERAGE MONTHLY MALICIOUS DOMAINS

18%

There are a couple of explanations for such dramatic growth.

- The overall number of malware and botnets, most notably Necurs and other ransomware-related malware, has grown significantly from 2016 to 2017. This goes hand-in-hand with the substantial increase in the number of cyberattacks seen this year.
- Existing botnets are transforming from using static IP as their C&C, which does not use DNS, to using domain names, which makes C&C servers more resilient to shutdown attempts by security firms. In other words, this is about an existing "install-base" of infected devices migrating or "upgrading" to a more sophisticated communication method.

CHART 1: **GROWTH IN MALICIOUS QUERIES FROM MARCH 2016 TO FEBRUARY 2017**



Summary of Attacks by Function

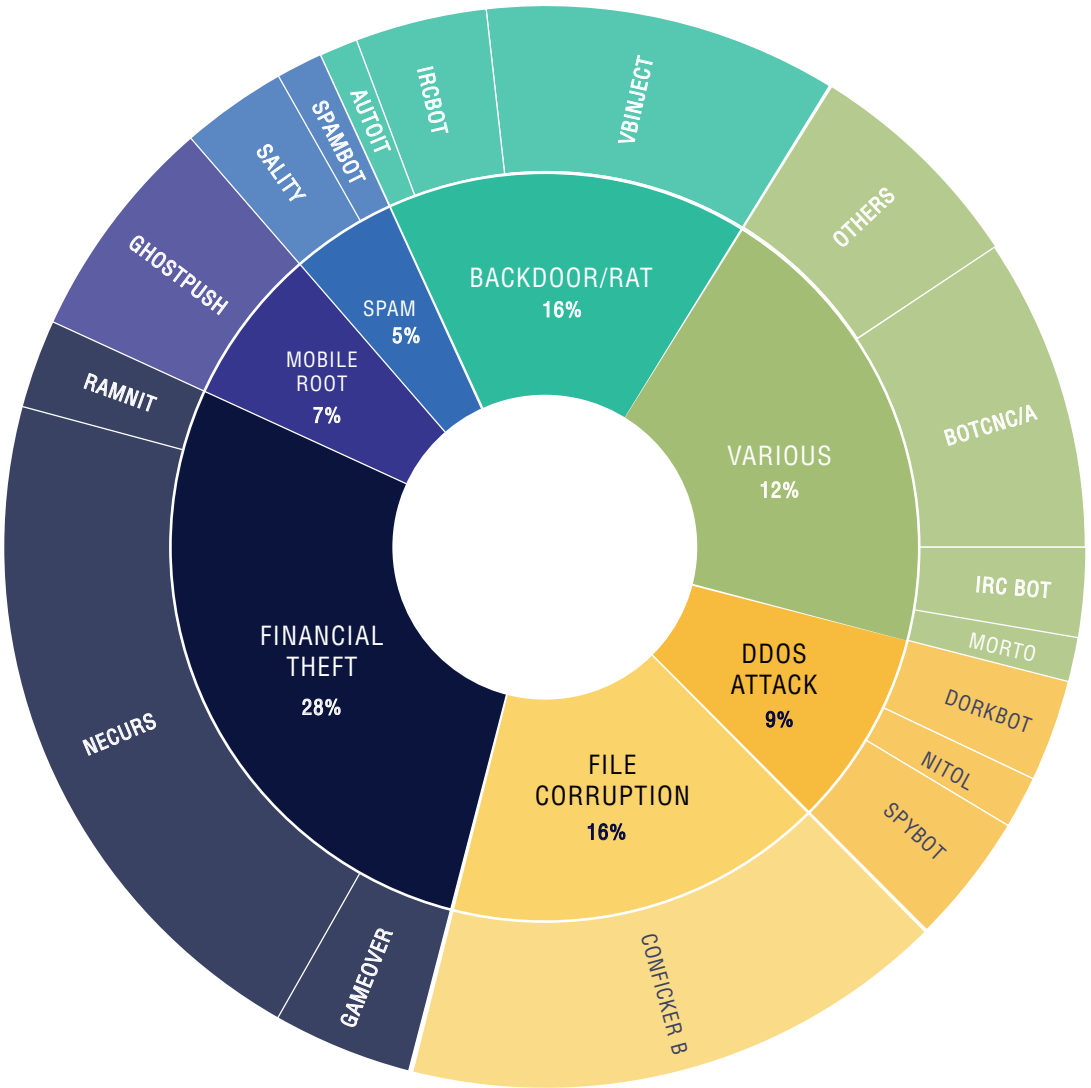
Nominum examined attacks by their prime function. While each type of malware and each botnet can serve multiple functions, at any time they have a main function that outweighs the others.

Most of the threats seen in our analysis are directly related to financial gains.

Chart 2 shows the main function groups we've seen during our six-month data set.

Most of the threats seen in our analysis are directly related to financial gains—whether they are ransomware, financial Trojans or click-fraud attacks. Looking at it from a "business" point of view, these are the types of attacks that generate the highest and fastest return on investment. And most attackers, as we've learned,

CHART 2: **TOP MALICIOUS QUERY SOURCES BY MALWARE FAMILY/TYPE**



are financially motivated. Take, for example, the CryptoLocker ransomware scheme which raised $325 million in 2015 alone.[2] Or Reveton ransomware that used cybercriminal gangs to extort over €1 million per year.[3] We also see various "traditional" malware and botnet activities still going strong—distributing spam, opening a backdoor for additional malware downloads, or pushing unwanted ads.

This is not the type of graph you would have seen ten years ago. The motivation for cybercrime has always been money, yet the level of effort concentrated at direct financial attacks has never been as elevated as it is today.

Why the Commercialization of Malware is Taking its Toll

The development of malware and attacker tools has been improving over the years, which is demonstrated in more complicated code, developed in larger amounts. When the dark marketplaces started selling malicious kits over 10 years ago there was a relatively small number of expert hackers at the top of the pyramid who created and sold tools or kits to the less tech-savvy criminals. Today, the expert hacker is the fastest-growing segment in the attackers' ecosystem, according to NSS Labs.[4] This means the size of the serviceable "less-tech-savvy criminals" segment can grow as well, especially now when DDoS attackers are available for hire for $5 an hour.[5] With more demand and more ability to fulfill this segment, motivation to quickly create more damaging and more sophisticated malware is high. This leads to mature development standards and a high degree of attack automation, and increases in the number of potential targets.

The motivation for cybercrime has always been money, yet the level of effort concentrated at direct financial attacks has never been as elevated as it is today.

Take for example the Mirai botnet, which automatically finds IoT devices and enlists them as "zombies" in a botnet army. Last fall, hacker Anna-senpai made the Mirai code open source so hackers could start developing different variants of the code to make the botnet more powerful. In February 2017, a U.S. college faced a Mirai-based DDoS attack that lasted 54 hours, a significant increase since most DDoS attacks last about 24 hours.[6]

The cybersecurity community started developing tools and techniques about 10 years ago in a different threat environment. The formula was to detect a malicious file, or family of files, reverse-engineer them and create a dedicated signature to block them. This approach was highly effective for the development speed in 2007. With the speed and sophistication of malware development in 2017, security teams are unable to keep up by using past-generation methodology.

The paradigm shift we've witnessed for the past few years has been the departure from the older, signature-based approach to security, to a heuristic, evidence-based approach. In a broad sense, the security world acknowledges that "unknown" threats are a given and that it is imperative to stop them, even if it means prioritizing speed over full certainty. As long as there is enough circumstantial evidence, threats, both named and unnamed, must be stopped.

[2] http://thehackernews.com/2015/10/cryptowall-ransomware.html
[3] https://www.infosecurity-magazine.com/news/reveton-ransomware-gang-busted-by-europol/
[4] https://media.blackhat.com/ad-12/Artes/bh-ad-12-cybercrime-kill-chain-artes-slides.pdf
[5] http://www.computerweekly.com/news/450296906/DDoS-attacks-openly-on-offer-for-5-an-hour-researchers-discover
[6] https://www.incapsula.com/blog/new-mirai-variant-ddos-us-college.html

1 PREPARATION

> "There is no shorter road to defeat than by entering a war with inadequate preparation."
>
> **CHARLES LINDBERGH**

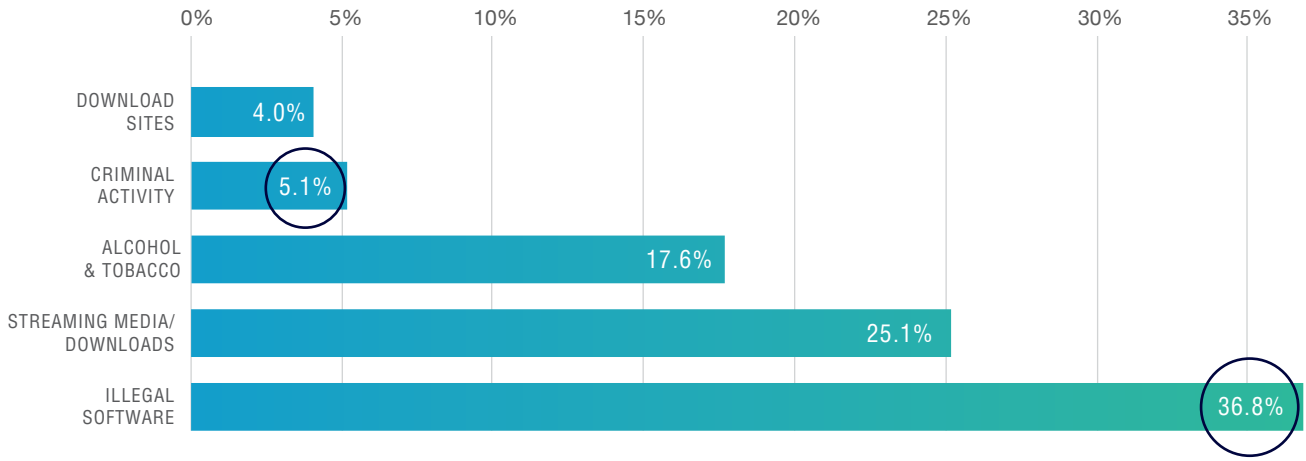
The term cyberwar continues to dominate the news headlines—from the U.S. election controversy to the North Korean nuclear threat and recent WikiLeaks revelations about government-sponsored hacking and espionage. One reporter from The Guardian recently declared that we might be living in the first world cyberwar.[1] Politics aside, and at the risk of oversimplifying the current, highly complex landscape, we prefer to view "cyberwar" in broad terms—as a war of good against bad, involving those who want a better, safer internet fighting those who use the internet for exploitation. Both sides require extensive preparation.

Now, getting back to our attack ladder metaphor: the first stage (or bottom rung) in the attack ladder is preparation. During this stage, the attacker is looking for vulnerabilities. Attackers harvest email addresses of potential victims, gathering information from social networks and often purchasing the exploits and malware that will deliver an initial payload. In some cases, open-source code will be downloaded and altered. This stage could take anywhere from a few hours to a few weeks, depending on the level of sophistication of the attack, which is entirely dependent on the ambitiousness of its goal. In an Advanced Persistent Threat (APT) attack, considered the most sophisticated attack type, the preparation stage could last months, as the attacker needs to have a full understanding of the target and the security mechanism protecting the target before he can create the dedicated malware pieces to hit the target.

The preparation stage is performed mostly underground and is exceptionally difficult to detect or stop. Some security firms and law enforcement agencies are trying to mitigate the "weapons proliferation" by finding and blocking exploits and malware "shops" around the net, typically closed forums or different Internet Relay Chat (IRC) channels often using TOR servers (also known as the Dark Web where communications are encrypted and essentially anonymous).

[1] https://www.theguardian.com/commentisfree/2016/dec/30/first-world-cyberwar-historians

CHART 3: **TOP CYBERCRIME CATEGORIES BLOCKED BY N2™ SECURE CONSUMER**



One in three content theft websites expose users to infectious malware, and website visitors are 28 times more likely to encounter malware on illegal download sites than on legitimate sites.

Success rates of blocking "weaponization" efforts are limited given the dynamic nature of attacker communities. One marketplace will be taken down and then another one will resurface the next day. Detecting reconnaissance is also a challenging task considering the number of different ways this goal can be achieved and the huge resources required to keep track of all the suspicious activities that happen on the worldwide web. The only actor who potentially has such huge resources is a large, state-sponsored organization (however, this topic is beyond the scope of this report).

Given the secretive nature of the preparation phase, DNS-level security (like all other network or endpoint security measures) does not have any visibility into the malicious preparation acts themselves. Blocking domains that are used to serve underground marketplaces is a place where DNS makes the most impact.

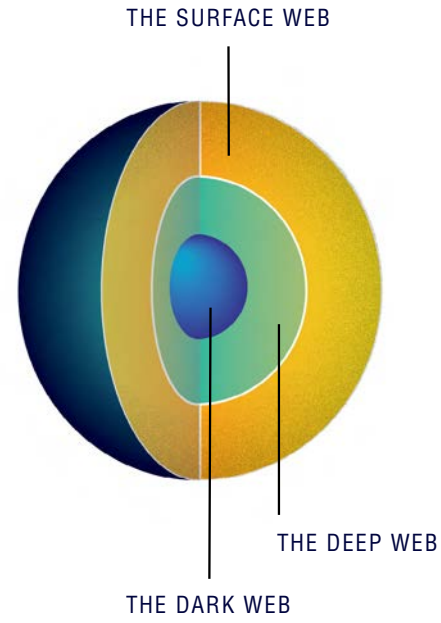
As seen in **Chart 3**, the criminal activity category, which includes primarily underground marketplace sites, represents on average 5.1 percent of all queries blocked by Nominum N2 Secure Consumer. (N2 Secure Consumer is a cloud-based solution that offers protection from phishing, ransomware and other malware, and also includes parental control options.)

Illegal Software sites, which often facilitate the download of tools required for hacking, are the most popular blocked category on the list. Not surprisingly, these sites are ideal hunting grounds for attackers. One in three content theft websites expose users to infectious malware, according to a report by Digital Citizens Alliance, and website visitors are 28 times more likely to encounter malware on illegal download sites than on legitimate sites.[2]

[2] http://www.prnewswire.com/news-releases/digital-bait-internet-users-at-high-risk-of-malware-from-content-theft-70-million-underground-market-300190959.html

Peeling Back the Onion

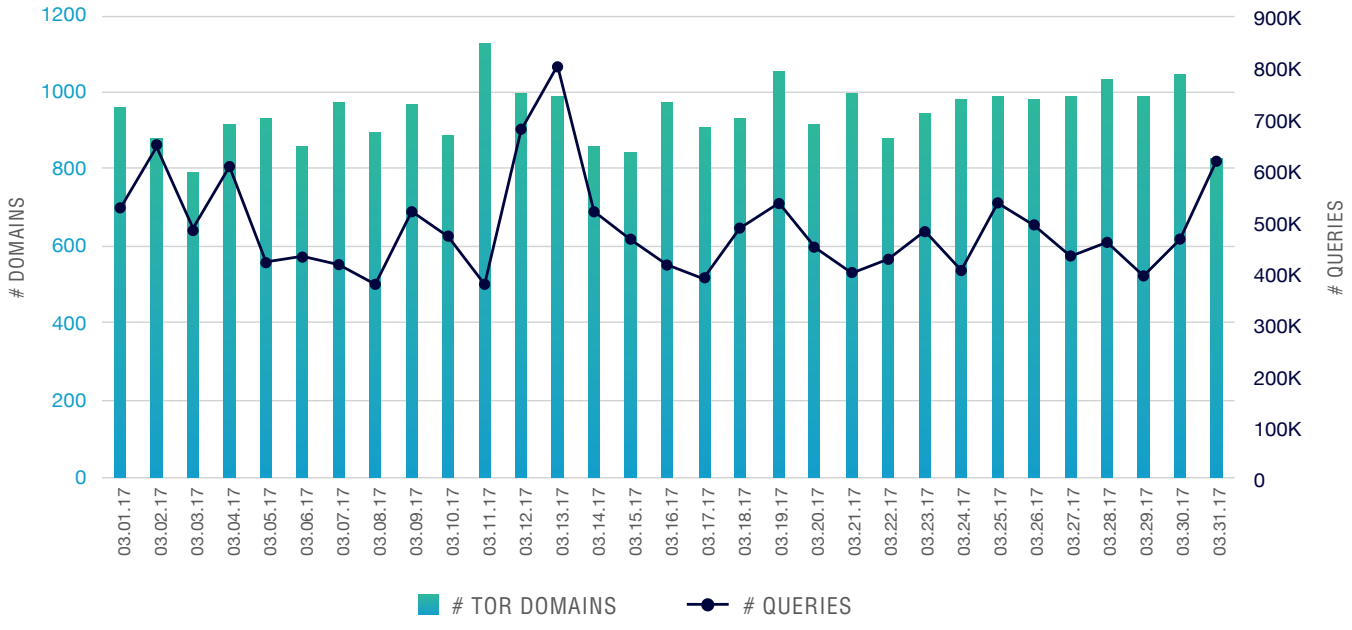
The internet has three levels. The surface level is the web we all know and use with web pages that show up in a search engine because they are indexed. The level beneath it is the deep web or the part of the internet that is not indexed by search engines. Then there's the dark web, where we find layered proxy networks, making privacy (and freedom levels) even higher and where special software is installed. TOR ("The Onion Router") is by far the largest and most popular of dark web browsers.



The high level of online anonymity and privacy provided by TOR makes it ideal for the cyber-community to prosper off the grid—but not completely. While TOR addresses (which use the .onion pseudo-TLD) don't use the DNS layer for browsing, many requests for .onion are seen in Nominum DNS data, either because users click .onion links outside the TOR browser (or other applications), or as a result of DNS leaks, which happen when operating systems continue to use default DNS servers rather than anonymous servers. **Chart 4** shows the number of unique suspicious TOR domains and the daily traffic seen by Nominum Data Science.

On average, we see 950 unique TOR domains and around 480,000 TOR queries per day. This sheds light on the level of activity in the dark web. It is somewhat harder to estimate the exact number of unique visitors to these sites, but based on data signals we estimate the number to be around 25 to 45,000 per day. This is possibly the size of the attacker base we need to stop every day. Some of the domains we see are dedicated links for making Bitcoin payments, where many of them are ransom payments created for ransomware victims.

CHART 4: **TOR DOMAINS AND DAILY QUERIES**



RANSOMWARE ATTACK LADDER

The Cyberattack Ladder provides an extensible framework from which we can dissect the component pieces of an attack. Here we use it to look into the stages of a ransomware attack from the bottom up.

ATTACK

ACTION

The ransomware encrypts valuable data file types on the user's device and presents "customized" messages such as how and when to pay.

C&C

After execution, the ransomware tries to communicate with its C&C server. If successful, the C&C sends a public key and corresponding Bitcoin address.

INTRUSION

INSTALLATION

Install ransomware on target device

EXPLOITATION

Leverage vulnerabilities such as Adobe Flash or Microsoft Silverlight as gateways to installation.

DELIVERY

Send phishing email. Include the weaponized payload as an attachment. Use social engineering to persuade users to open file.

PREPARATION

WEAPONIZATION

Acquire an exploit kit such as Angler, Neutrino, or Magnitude to get an easy-to-use, zero-day vulnerability exploit. Couple it with malware such as Cryptowall or Cerber. Test anti-spam and anti-virus evasion.

RECONNAISSANCE

Harvest email addresses of potential target and victims; gather information from social networks and other public sources.

// TECH NOTES

From "New Core Domains" to "Zero-day Attacks"

Nominum Data Science has a recipe to classify new domains. First, we filter new domains into a quarantine list or "gray list." Then, additional classification algorithms are used to make the distinction between gray-area domains and legitimate domains.

Next, we group domains that have resolved DNS queries and the domains that have unresolved queries. This is important for our threat classification: new, unresolved domains are usually associated with botnet C&Cs. New, resolved domains are associated with phishing, adware, malvertising and other types of attacks, which must be registered and resolvable to perform their intended malicious function.

The Nominum Zero-day Dashboard provides a real-time, inside view into the process of detecting new malicious core domains. We begin with one million queries processed per second, then filter for new core domains only (usually 50-60 per second). Then, Nominum machine learning algorithms are applied, along with filtering and clustering to identify malicious domains. On average, four to five percent of domains reach the end of the funnel, and are relayed to our streaming threat intelligence.

Once the domains are classified into two mega-groups, Nominum Data Science applies proprietary (unsupervised) machine learning algorithms to build smaller clusters of domains, identifying subtle relationships between the cluster's members to glue them together. Now that we have our new core domain clusters, we move to final classification. We want to determine "known/named-malicious" or "unknown/unnamed-malicious" queries.

We match our clusters with up-to-date third party cyber-intelligence data. If even a single domain in a cluster is mapped to one of the "known" malicious domains, this elevates the maliciousness level of the entire cluster (what we call "guilt by association"). The more domains we can map in a cluster to "known" malicious domains, the higher our confidence is in the maliciousness of the cluster.

Next are the "unknown/unnamed-malicious" clusters. In this category, we consider the clusters that do not match any known threat but still have enough bad characteristics to indicate maliciousness. A cluster of unresolved domains, e.g., those with a similar string length, are very likely malicious, even though the security industry has not yet identified and named them.

As mentioned earlier, the enormous growth in the number of cyberthreats, powered by the commercialization of malware production, tests the limits of security firms. How can they survive the cat-and-mouse game against attackers without exhausting resources? Rather than hiring thousands more researchers and analysts—a good, yet expensive idea—Nominum takes a leap of faith into the threat-agnostic approach where threats are detected and blocked without prior knowledge about them based on anomalous behavior. This is accomplished with the unknown/unnamed-malicious clusters classification.

The examples below show the extent to which our Zero-day Quarantine method helps stretch existing cyberthreat intelligence. All data is based on a single day of analysis.

In **Chart 6**, you see quarantine Cluster 25 which was created through the Zero-day Quarantine clustering process on March 19. It includes seven core domains. When matched against third party cyber-intelligence, one of the domains in the cluster was found to be related to a recent C&C activity of a specific threat type. Based on this information, we use the "guilty by association" approach, elevating the risk level of the other six (never seen before) domains.

CHART 5: **NOMINUM ZERO-DAY QUARANTINE DASHBOARD**

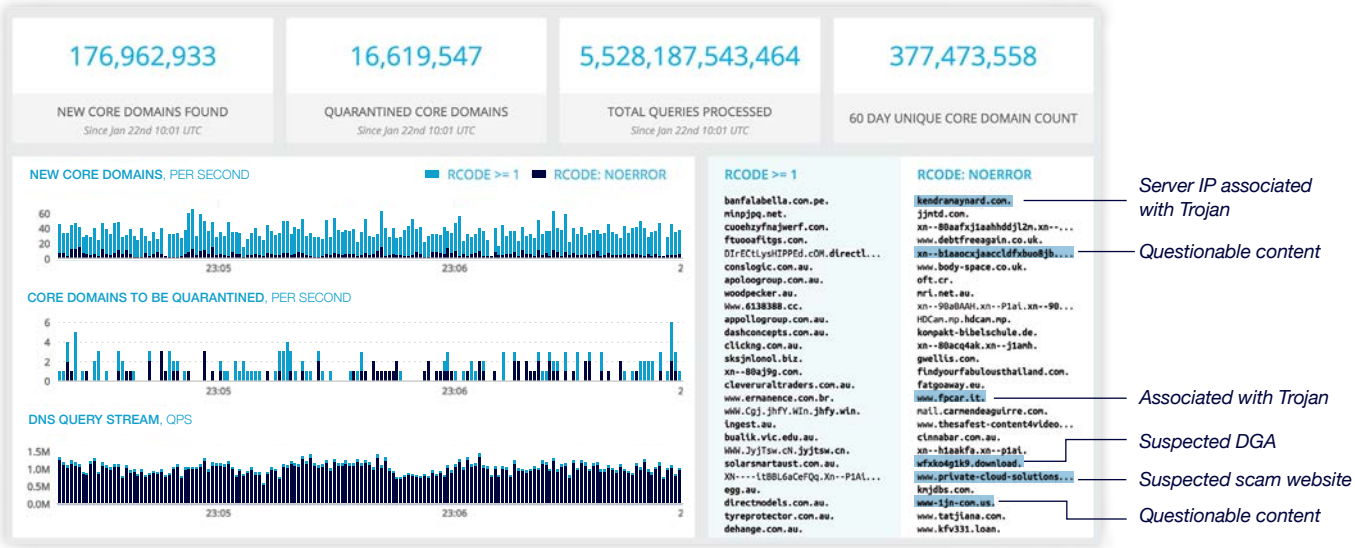


CHART 6: **CLUSTER OF SUSPICIOUS DOMAINS**

·····	domain-a.com	domain-b.com	domain-c.com	lnhmm.com ·····
·····	domain-c.com	4bhkflats.com	domain-c.com	domain-b.com ·····
·····	domain-d.com	agroworkz.com	agroworkz.com	domain-c.com ·····
·····	scotthwalters.com	domain-a.com	domain-d.com	domain-c.com ·····
·····	domain-c.com	domain-b.com	studentreceptionist.com	domain-b.com ·····
·····	domain-b.com	superradatorcoils.com	domain-d.com	domain-a.com ·····
·····	domain-a.com	domain-c.com	domain-b.com	erinisthebest.com ·····

Nominum machine learning and clustering methods uncover malicious patterns. Each line is a sequence of DNS queries. The domain names in the blue boxes are part of Cluster 25. Clusters are determined by domain names appearing in a similar context.

2 INTRUSION

> “Is then no nook of English ground secure
> From rash assault?”
>
> **WILLIAM WORDSWORTH**

The famous English poet William Wordsworth, a staunch conservationist, rallied against a proposed railway in the English countryside as he wondered what damage it might cause to the environment. When it comes to intrusion on the worldwide web, no nook or geography is immune to attack. The global village that is enabled by technology also means that attackers can strike anytime and anywhere.

The goal of the intrusion stage is to deliver the weapon to a victim’s device, exploit a weakness in their system (an exploit that was researched in the preparation stage) and then install malware onto the device. By the end of this stage, the attacker is ready for the final stage, the attack, where the ultimate goal of the attack is accomplished.

There are various techniques used today by attackers to accomplish each one of the delivery, exploitation and installation steps in the intrusion stage. In this section, we will take a look at some of the most prominent techniques to learn how DNS-based security methods can help mitigate these threats.

Phishing for Victims

The most common method of delivering a “weaponized” payload to a potential victim is through phishing, or, in a more general term, social engineering. Phishing has evolved over the years from a term used to describe an attempt to deceive a user into revealing their credentials by creating an email message and website that resembles an online banking or payment system.

Today, the term phishing describes the art and science of luring a user into clicking a link on a visually-trustable message that leads to a malicious drive-by download site, or into opening a malicious yet benign-looking attachment in an email, or a link in a text message or social media post.

Clicks on phishing message links, whether they direct a user to a fake banking site or a drive-by download site, go through the DNS layer and are therefore represented in DNS data. An attacker who tries to test a nefarious site before mass-distributing the phishing email can also be identified in DNS. Nominum Data Science has a unique perspective into the phishing delivery process because DNS can identify "patient zero" of an attack and block future would-be victims as they unknowingly attempt to access the phishing site.

Chart 7 displays the average length of phishing attacks. We selected 900 domains of some of the top phishing targets (there are typically over 100 unique domains per target) and measured the time from the second a domain first appears in DNS data to when it no longer directs a victim to a landing page. Our results show that on average a phishing site stays alive for 1.5 days.

A benefit of using DNS data for phishing detection is its visibility into the exact number of unique visitors to a phishing domain. Rather than observe the number of phishing emails detected in a single network (by using an anti-spam filter), DNS data tells us who clicked on a malicious link and provides a better overall intrusion assessment.

Also, malicious links that phish the user on social networks or mobile devices are invisible to traditional anti-spam and anti-phishing filters, yet can be seen in DNS traffic.

Analyzing a few hours of a phishing site activity, Nominum Data Science reveals the following pattern:

Almost 100 percent of users who clicked the malicious links did so in the first five hours of the attack. Sample malicious domains include:

- 9irequest-redirect
- 20apple.manage84istore.co.uk
- commbank.netbank-personal.com

The main lesson is that the impact of a phishing attack occurs within the first five to 10 hours from launch. Therefore, mitigation of a phishing attack is extremely time-sensitive. If anti-spam filters fail to block the phishing email (either because a new type of email has been sent, or because the message is not in the form of an email), it is important to have another security layer to block the phishing domains themselves.

CHART 7: **PHISHING ATTACK LENGTH**

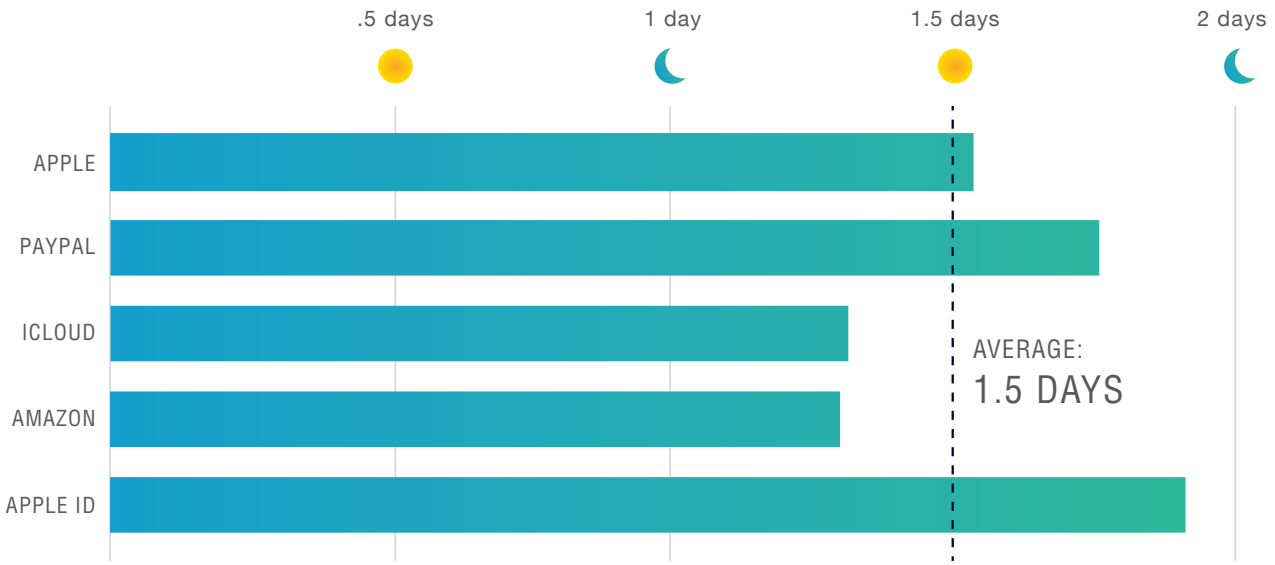
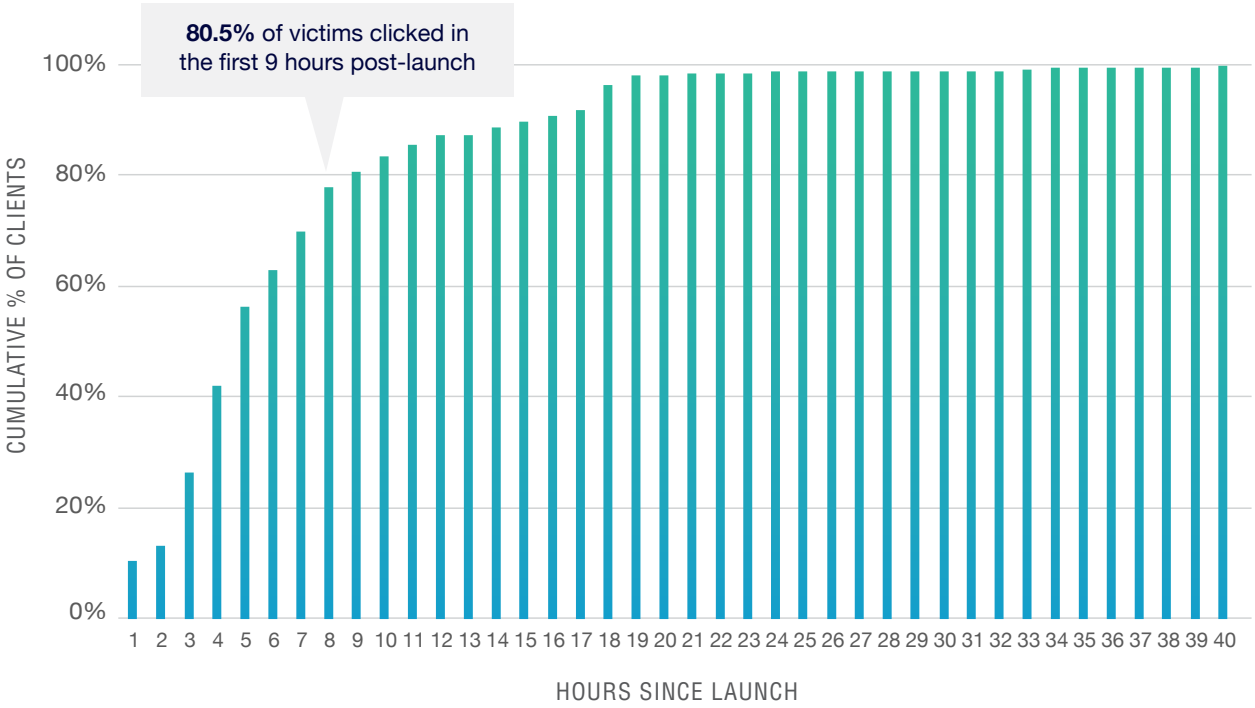


CHART 8: **CLIENTS PHISHED PER HOUR IN A SAMPLE**

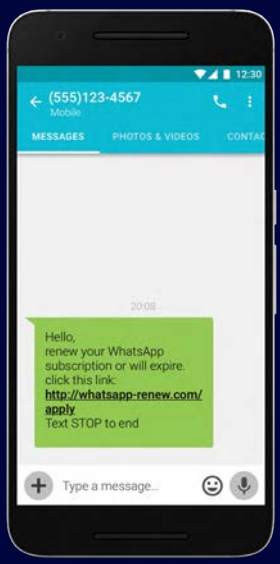


WHATSAPP PHISHING

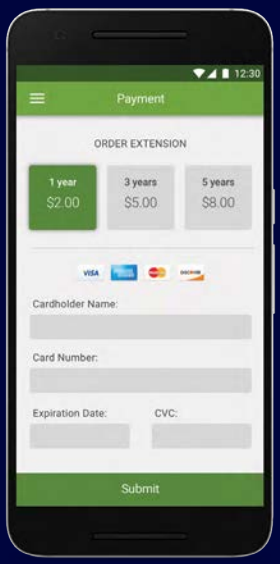
WhatsApp is one of the most popular cross-platform messaging apps in the mobile world, with over a billion users worldwide.[1] It has also become a target of phishing attacks. In the example below, text messages include a malicious link that urges users to "renew WhatsApp subscription" or pay a fake bill. When clicked, a mobile web page asks users for credit card information.

While most mobile device management solutions don't look into instant messaging contents, mobile devices can be protected by the DNS layer. Once a user clicks the link in the phishing message (in the above screenshot, the target was one of our Data Science team members), the domain query reaches a DNS server (supported by a DNS security platform), which identifies it as malicious, and therefore returns an NX response code (e.g., domain name does not exist). The user cannot reach the phishing site, and the attack is blocked.

[1] http://www.deccanchronicle.com/technology/in-other-news/191116/whatsapp-scams-all-you-need-to-know.html



1. User receives a text message to renew their subscription



2. Clicking the link sends the user to a fake payment page asking for credit card info.

Malware Download Sites

Phishing as an intrusion vector is usually coupled with malware-downloading sites. These sites, which can host various malware files, are accessed through a user click on a malicious link embedded in a phishing message, or, alternatively, a click embedded in a dangerous site (adult content or file sharing sites usually fall into this category). In turn, this click facilitates the actual download of a malicious file onto the user's device.

Drive-by-downloads

The other way of downloading malware that requires less user involvement (and is therefore considered a more deceitful approach to intrusion) is called a drive-by-download. Drive-by-downloads typically work without user action by exploiting a vulnerability in the user's browser or a browser plug-in that they've downloaded. Often, this is done by redirecting subscribers to sites hosting known exploit kits.

With this method, a user needs only to pass through (i.e., visit a web page without clicking or accepting any software) and malicious code is downloaded to the user's device in the background. A drive-by site can be a legitimate site that was compromised by an attacker, causing it to host several different types of malicious code that the attacker hopes will match a weakness on the user's device.

Chart 9 shows the number of queries directed to malware-downloading sites over a single day, as seen in data from Nominum N2 Secure Consumer. For instance,

Nominum Malware Download Sites Blocking Stats

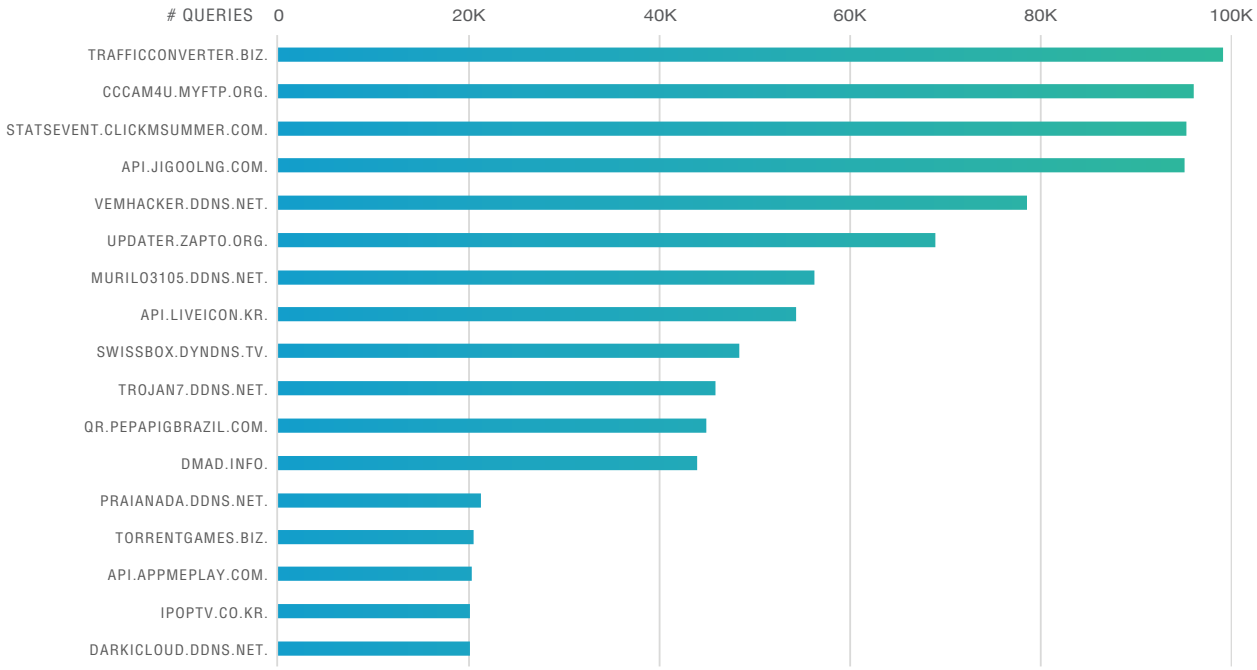
DIRECT MALWARE FILES LOCATIONS BLOCKED:

404,387

TOTAL URLS OF MALWARE DOWNLOAD SITES BLOCKED:

~2 million

CHART 9: **TOP MALWARE DOWNLOADING SITE QUERIES - ONE DAY SAMPLE**

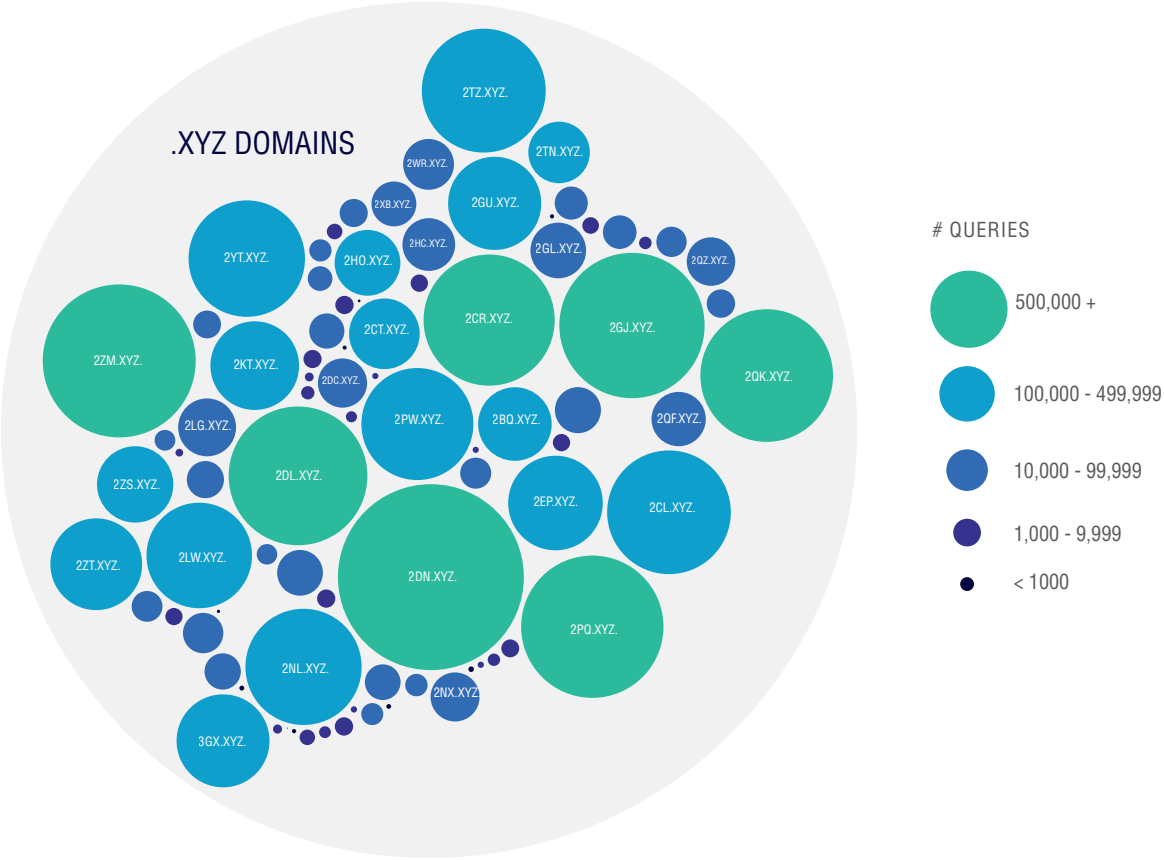


api.jigoolng.com, a site related to Android malware downloads, was queried by over 10,000 devices in a single day. Trafficconverter.biz, a downloading site with 100,000 queries, is known to be one of the top 10 most malicious sites in Tunisia (queries are generated from around the world). Dmad.info is a known drive-by-download site for which we've identified over 40,000 queries from over 1,000 devices. Overall, a query seen to any of these sites indicates that an intrusion attempt is in the works. Rather than hope that the user's anti-virus software will pick up the specific malicious code once it tries to download, our approach is to block the traffic at its source and not allow the download to happen in the first place. Nominum actively generates global threat lists to block over 100,000 malicious domains daily.

Visiting a drive-by-download site can also be triggered by a redirection from the site the user originally attempted to visit, or through a pop-up window in the originally requested domain. One place to see this attack vector in the DNS layer is to crawl through suspected phishing domains and identify common patterns. In the example below, we detected a malicious re-direction family of domains, all following the name pattern 2**.xyz and affecting mainly adult content sites.

Over a period of 48 days, we observed 173 domains. At the time this report was written, the number of queries to these domains stood at 10.3 million, originated by over two million devices. All domains above are blocked by N2™ Secure Consumer.

CHART 10: **MALWARE DOWNLOADING SITES WITH .XYZ PATTERN**



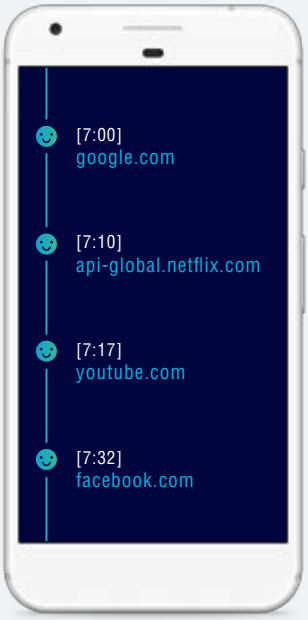
Exploitation and Installation Steps

The initial malicious file downloaded by the user is typically quite small (a method to evade the risk of detection by a network firewall, IPS/IDS or endpoint anti-virus). Once on the user's device, the malware exploits a vulnerability (identified in the preparation stage) to execute the malicious payload. Technically, this usually happens by running a DLL injection to gain administrative privilege on the compromised machine.

From this point forward, the attacker holds a covert channel to receive commands, download additional files and launch attacks from the compromised device.

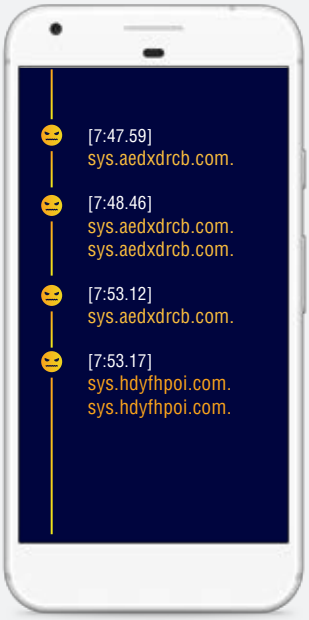
AN HOUR IN THE LIFE OF AN INFECTED DEVICE

Still a healthy, safe device (although dormant malware is possibly already hiding on it), the phone makes internet API calls to popular web sites, including **Google, YouTube** and **Facebook**. We assume this device is not compromised.



At 7:43:40, things turn malicious, with a query to **m[.]aedxdrcb[.] com**, a Fully Qualified Domain Name (FQDN) known to be an indicator of a Ghost Push attack. In the 59 seconds, the device tries to contact this FQDN seven additional times.

Three minutes pass after this single query, a new wave of malicious queries begins with three queries to **sys[.] aedxdrcb[.]com**, then three more similar queries occur in a span of five seconds.



So, what just happened? First, it is likely that the user has downloaded a compromised/malicious app to their device, or they visited a compromised website at some point in the day, most likely adware-related. That activity went undetected by any of the device's endpoint security mechanisms. The initial infection collected information about the device, and tried to post it to aedxdrcb[.]com. Next, it likely tried to download a malicious APK from syllyq1n[.] com. If this APK download is successful, it roots the victim's phone.

Luckily, the device's user was on a network protected by N2™ ThreatAvert, which shields networks from threats that originate from within it. N2 ThreatAvert blocked all attempts to communicate with the attacker (e.g., receive commands or send data) stopping the complete takeover of the device from happening.

Pumping and Dumping: A Tale of the Necurs Botnet

One of the trends we've seen in the past six months is the incremental growth in Necurs botnet activity. As mentioned in the Fall 2016 Data Revelations Report, Necurs was used throughout 2016 as the channel for distributing Locky, the top ransomware of 2016, and Dridex, one of the top financial Trojans of the year.

As we well know, a botnet army for hire receives a task, and then executes it—no questions asked. After its great success in the financial threats distribution business, Necurs has taken a new role in 2017: distributing pump and dump spam campaigns. Pump and dump is an old penny stock price manipulation scam, yet Necurs breathed new life into it with a new level of aggressiveness.

Pump and dump schemes target penny stocks that trade in very limited volumes. This thin trading volume means that a small increase in demand for the stock can lead to a rapid increase in price. Falsely "recommending" a large group of potential investors to purchase the penny stock, via spam emails, can lead to a quick spike in stock price, followed by an equally quick downfall. Hiring a spamming botnet as large and powerful as Necurs means a greater chance of success for the scam organizer, and higher monetary gains (and monetary losses on the part of the scam victims).

If you've watched the movie or read the book *The Wolf of Wall Street*, this is the real-life technique used by Jordan Belfort (played by Leonardo DiCaprio in the movie).

One of the recent stocks affected by the Necurs-powered pump and dump scam was that of the media holding company inCapta (INCT:OTC). Over three trading days in March 2017, inCapta's share price went up from 13 cents to 18 cents a share or nearly 40 percent growth.[2] This growth was driven by a stock recommendation spam campaign orchestrated and distributed by the Necurs botnet. The stock price dropped to 10 cents a share the next day, once the perpetrator sold all of his shares in peak price.

CERBER RANSOMWARE

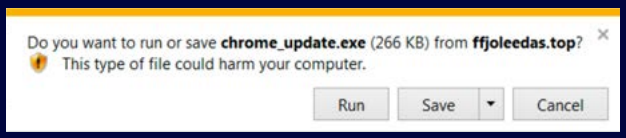
Six months after Locky claimed our "top ransomware" award, it appears that 2017 has a new leading candidate to the title. Cerber has been around since early 2016, yet needed a few improvements to its evasion technique and a different business model to make itself the "ransomware of choice" for many attackers.

Since the beginning of the year, Nominum Data Science has followed Cerber through its various stages—from infection domains, to its C&C domains, and, finally, to the post-infection traffic, which involves Bitcoin payment transactions between the victim and the attacker.

The Cerber ransomware infection happens either via a spam (or a Malspam) email with a malicious attachment (.zip or .js file) or a malicious link, which redirects the victim to a fake Google Chrome update page. Some of the active infection domains we've seen in March were:

chromefastl[.]top
chromehakc[.]top
ffjoleedas[.]top
newsectorbs[.]top

The .top Top Level Domain (TLD) is frequently used by Cerber as seen on the screen shot below.



Blocking Cerber in the intrusion stage is possible at the DNS level, and can save heartache and money. By blocking users from reaching Cerber infection domains (as we do with the N2 Secure Consumer application) to download the initial ransomware file, one can stop the attack before it takes over a user's data and it doesn't cost a lot to do so.

[2] http://blog.dynamoo.com/2017/03/pump-and-dump-spam-incapta-inc-inct.html

3 ATTACK

> "We are now living on internet time. It's a new territory, and the cyber equivalent of the Oklahoma land rush is on."
>
> **ANDY GROVE**

After days or weeks of preparation, and a few minutes of actual intrusion, the attacker is now ready to launch the attack. The user's device is running the attacker's malicious code, awaiting further commands. In this section, we discuss the ways commands are passed to the compromised device, the types of consequent attacks, and finally, how DNS security tools and intelligence can be used to stop or mitigate the attack risk.

The first thing to keep in mind: when we talk about a "compromised device" in 2017 we're talking about a wide surface area. From laptops to smartphones to smart devices, almost every type of smart device can be compromised and can be part of a cyberattack. In the past, the key solutions for the active attack stage would have been anti-virus software and app controls. In a world where many of the devices are smart devices, which are, in fact, not as smart as a laptop, this approach doesn't work.

The second thing to keep in mind: a compromised device is, in fact, a device that runs the equivalent of a covert, malicious, parallel operating system. This operating system is controlled by the attacker and, getting its command remotely from him, in turn, controls some of the device resources. In other words, where a benign OS is commanded by the legitimate user to open applications like MS Excel, the malicious OS is commanded by the attacker to, for instance, encrypt the device's data.

Here are some malicious activities a compromised device can perform:

- Distributed Denial of Service (DDoS) attacks
- Steal data
- Take over online financial accounts
- Encrypt drives
- Send spam

BOTNET BREAKDOWN

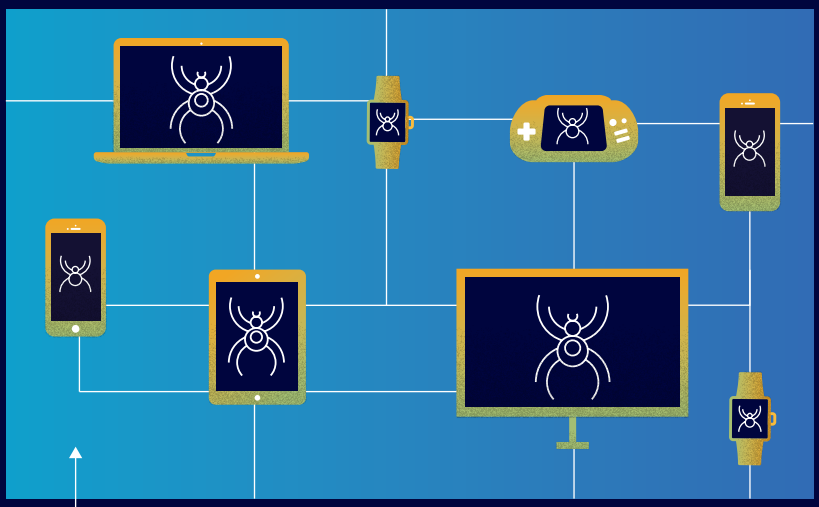
Most modern botnets rely on DNS as the service for location of C&C infrastructure. Nominum Data Science can discover and block C&C domains, which has an enormous negative impact on the stability and effectiveness of entire botnets.

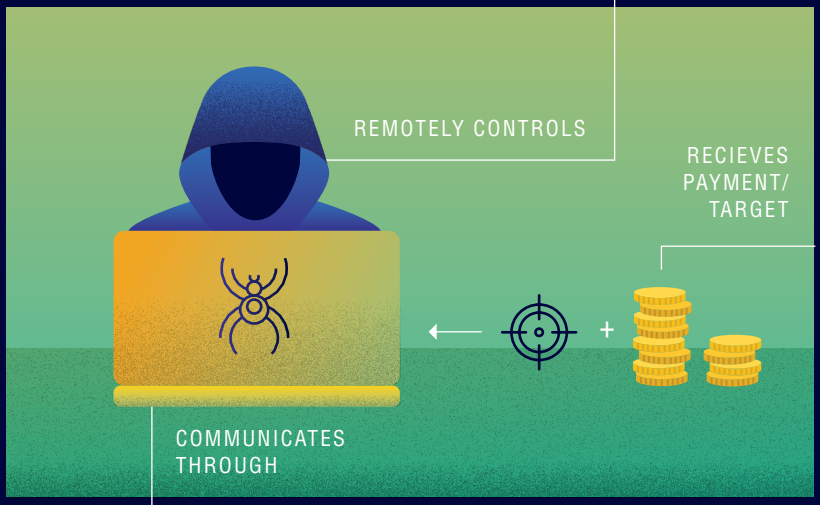
BOT/ZOMBIE:

An individual infected device within the botnet. The bot is connected to its botnet through a command & control server, and typically has no association with other individual bots in the same botnet. This way, if a single bot in the botnet is detected, it cannot divulge its partners in crime so the botnet remains unaffected. It is important to note that a bot can be a computer, a mobile device, or, as seen lately, any IoT device. The term zombie is a synonym to bot, where the image is of a body (device) controlled by a remote soul (attacker).

BOTNET

A botnet is a network of malware-infected devices. All devices in the botnet are infected with the same type of malware. Therefore, the botnet often 'inherits' the name of the malware. The botnet is an army to hire, which can perform multiple different activities for the right price. Popular activities are DDoS attacks, spam distribution and malware distribution.

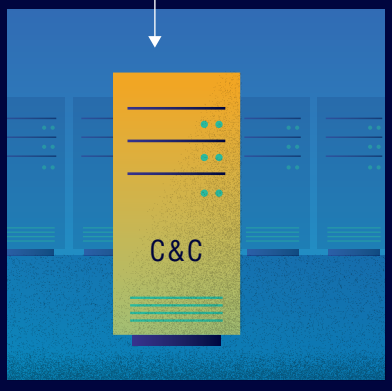




ATTACKER

A.K.A. CYBERCRIMINAL/BOT MASTER/BOT HERDER

The Attacker is the botnet operator. This is the individual who remotely controls the botnet and can send attack commands to all or some of the individual bots. A botnet attack will always start with the attacker. However, the mastermind behind a cyberattack may be the individual who hires the botmaster and provides the target for the attack.



COMMAND & CONTROL SERVER

A C&C (or C2) server is the central channel through which a bot communicates with its bot-master. This is the central computer through which commands are sent from the attacker to the bots in the botnet, and information is sent back from the bots to the attacker. Most botnets use a client-server architecture, and employ a range of alternative C&C topologies, each designed with "botnet security" in mind, optimized to minimize network activity (which may help security solutions to discover it) and withstand system failures.

It also gives the attacker access to the device and its connections, at which point it can start moving laterally to additional devices and resources on the network.

One thing common to almost all types of malware in the attack or breach stage is their interaction with C&C servers to receive commands or to extract data. This communication is detected through DNS traffic, so DNS security tools can be deployed to block it. While it's not the only C&C method, DNS is the most ubiquitous and easy-to-integrate network sensor to detect malicious C&C communication worldwide (and then apply it to any internal network).

In this chapter, we discuss some of the attacks we see in the active attack stage and share our data analysis results around them. But first, let's start by understanding the basics of malware communications, the common foundation for all attack types.

What Mirai Protection Really Means

The IoT botnet known as Mirai turned nine months old in April and has made quite a name for itself in its short life. Mirai was first seen active in its DDoS attack against the Krebs-on-Security website in September 2016, followed by a high-profile attack in October 2016 on the service provider Dyn which affected the accessibility of sites like Netflix, Twitter, Airbnb and New York Times. In late November, Mirai bots attacked a large network operator in Europe, causing a large-scale internet outage to hundreds of thousands of internet subscribers.

The botnet is constructed by scanning the internet for vulnerable IoT devices, hacking them and infecting them with malware so they can communicate with command and control (C&C) servers. Once an army of IoT devices is compiled, cybercriminals launch devastating DDoS attacks that cripple web domains by flooding them with queries.

Is today's Mirai the same Mirai we saw in 2016? The answer to some extent is "no." Mirai's source code was published in a hacker's forum in September and later in the month to GitHub, and has since been altered and adapted by hundreds of different malware authors around the globe for different purposes. So, if Mirai today is not the old Mirai, how do you know if you're protected?

// TECH NOTES

The early Mirai detection method, which many security firms have taken, is reverse-engineering the binary for C&C names and publishing these names. If you look at the open source code below, you'll notice that there is a pattern of 32 characters, which includes letters and numbers in sequential order. Now, anybody could download the source code, change the pattern and hope to evade detection. We saw some examples of this, as evidenced in **Chart 11**.

We developed a new generation of PRSD detection, which is based on behavioral attack features such as the number of unique subdomains, to detect a true PRSD attack.

While it was easy to detect this type of DDoS attack based on that pattern, at Nominum we realized before the open-source code was released that this will not hold forever for this type of attack; as mentioned in the report's introduction, attackers "follow the ladder" and failure to bypass security measures at any stage in the attack is their cue to make changes and find better ways to evade security. Thus, we took a proactive approach and developed a new generation of PRSD detection, which enabled us to detect PRSD-C (based on a sub-domain count method) while observing the Mirai C&C names from DNS traffic. This means we're now indifferent to any changes to the Mirai source code, or to any other PRSD-type code.

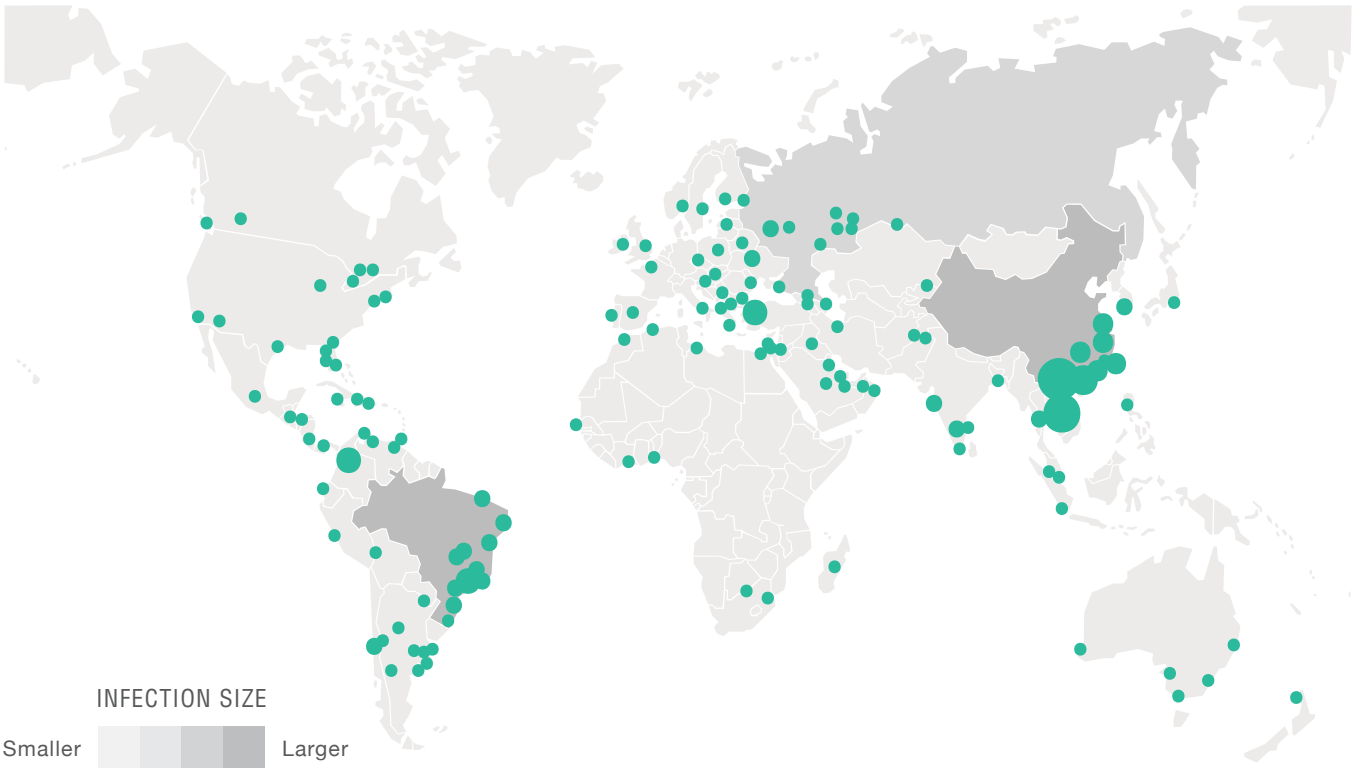
CHART 11: **MIRAI SOURCE-CODE**

```
{
    const char alphaset[] = "abcdefghijklmnopqrstuvw012345678";

    while (len > 0)
    {
        if (len >= sizeof (uint32_t))
        {
            int i;
            uint32_t entropy = rand_next();

            for (i = 0; i < sizeof (uint32_t); i++)
            {
                uint8_t tmp = entropy & 0xff;

                entropy = entropy >> 3;
                tmp = tmp >> 3;

                *str++ = alphaset[tmp];
            }
            len -= sizeof (uint32_t);
        }
        else
        {
            *str++ = rand_next() % (sizeof (alphaset));
            len--;
        }
    }
}
```

Right shifts of 3 bits from an 8-bit number (highlighted in green) means that the result is between 0-31 characters, which corresponds exactly to the 32-character string above.

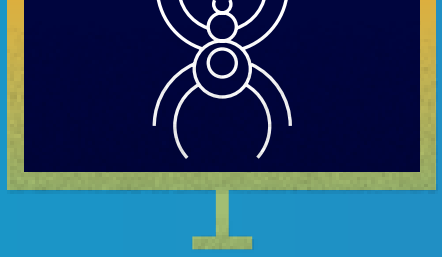
CHART 12: **LOCATIONS OF MIRAI-INFECTED DEVICES, WORLDWIDE**

Source: Nominum and 360 Labs



High concentrations of Mirai-infected devices are currently located in South America and parts of Asia, yet Mirai is causing damage on a global scale as seen here. The green circles represent the size of the infection of each city (by service provider).

The devices most vulnerable to Mirai are home routers, DVRs and internet-connected remote cameras, largely because these devices typically don't have the appropriate security software installed to protect them from the malicious botnet, and usually have external access enabled that is exploited by Mirai. Additionally, consumers often use the factory-default security passwords, which are easy for hackers to break through.



EXPERT COMMENTARY:

ANALYZING DNS LOOKUPS FOR PREDICTION AND DETECTION OF IOT ATTACKS

Nick Feamster, Princeton University

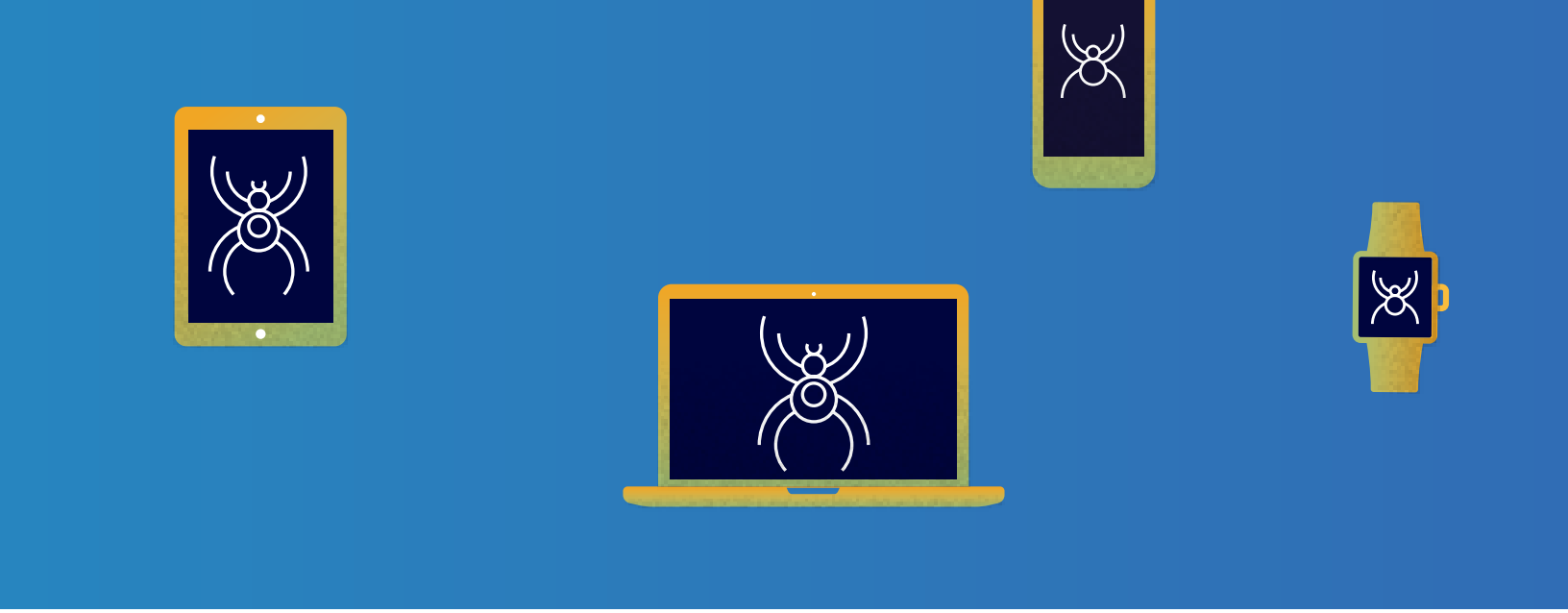
Nick Feamster is a professor in the Computer Science Department at Princeton University and the Deputy Director of the Princeton University Center for Information Technology Policy (CITP). Before joining the faculty at Princeton, he was a professor in the School of Computer Science at Georgia Tech. He received his Ph.D. in Computer Science from MIT in 2005, and his S.B. and M.Eng. degrees in Electrical Engineering and Computer Science from MIT in 2000 and 2001, respectively. Nick's research focuses on improving the security and performance of communications networks with systems that draw on advanced Internet measurement, data analytics and machine learning.

The proliferation of internet-connected devices—the so-called "Internet of Things" (IoT)—presents significant potential to change the way people live, work, and play; it is also poised to reshape how enterprise and industrial infrastructure is operated and managed. These internet-connected devices range from kitchen appliances, entertainment systems, and home security systems in the "smart home" to heating, electrical, and industrial control systems in large enterprise networks. These devices and their associated applications, unfortunately, bring with them an array of security vulnerabilities resulting from insecure software that in many cases may be difficult or impossible to patch. Although there are steps that we can and should take to protect them.

Our research in the lab at Princeton University has shown that the Domain Name System (DNS) can be a useful early indicator for attacks. Specifically, our research discovered that newly registered DNS domain names that are used as part of attacks often see large volumes of DNS lookups much earlier in their lifecycle than legitimate domain names. Observation and analysis of early DNS lookup patterns can often reveal the presence of attacks before they occur. For example, our research shows that the DNS domains used in attacks can receive lookups from thousands of unique networks within just a few days of the domain name being registered. Other signals, such as the infrastructure that hosts the authoritative nameserver for the domain—and how that hosting infrastructure evolves over time—also serve as effective predictors of many different types of attacks.

In IoT deployments, ranging from smart homes to enterprise networks, these DNS lookup patterns can serve as particularly strong signals for attack prediction. Many of the devices that we have examined in the lab—ranging from smart thermostats to internet-connected cameras—tend to only communicate with a small number of internet destinations as part of normal operation.

This specific behavior follows from the relatively narrow set of tasks and operations that a typical IoT device performs. For example, a smart light switch has a much more limited set of functions as compared to a general-purpose computing device; the more limited set of actions is reflected in a smaller set of DNS lookups. The typical smart home IoT device, for example, performs DNS



lookups to only a handful of predictable domain names (mostly associated with the manufacturer of the devices); deviations from this behavior may indicate an attempt to communicate with third parties ranging from attackers to advertisers. Monitoring DNS data for these types of aberrations can serve as an early indicator for attacks against the IoT devices themselves, as well as the internet at large.

Another important aspect of securing IoT networks is determining the devices that are connected to the network; in short, smart home users and network operators for large enterprises alike need better ways to inventory the increasing number of devices that are connected to their networks. DNS lookups also serve as a valuable signal for cataloging and tracking the devices that are connected, for several reasons. First, the DNS domain names that each device looks up are often clear indicators of the device itself; for example, we observed that one manufacturer of health tracking devices embeds the type of device (e.g., iPhone, desktop client, Android, etc.) into the subdomain of a DNS lookup to the manufacturer's top-level domain. Such DNS lookup information can provide important clues concerning the presence of IoT devices on the network, as well as whether the behavior of these devices changes over time due to compromise or malfunction. Second, we have found that the DNS lookups to the domain names corresponding to device manufacturers are often periodic, with DNS lookups to the manufacturer domain name occurring (say) once every hour. Because each IoT device in a collection of devices may perform these lookups out of phase from one another, it is often possible to count the number of unique devices of a certain type on the network simply by analyzing the periodic DNS lookups that occur on the network. Deviations from this periodic behavior can also suggest a security incident or a device failure or malfunction.

Observation and analysis of early DNS lookup patterns can often reveal the presence of attacks before they occur.

RECOMMENDATIONS:

1. Keep an inventory of IoT devices.

2. Look for anomalous behavior—most devices should only go to manufacturer sites.

3. Track the number of lookup attempts each device is making.

In the six months since we released our last report, we've seen PRSD attacks active daily, with an average of 706 million queries per day.

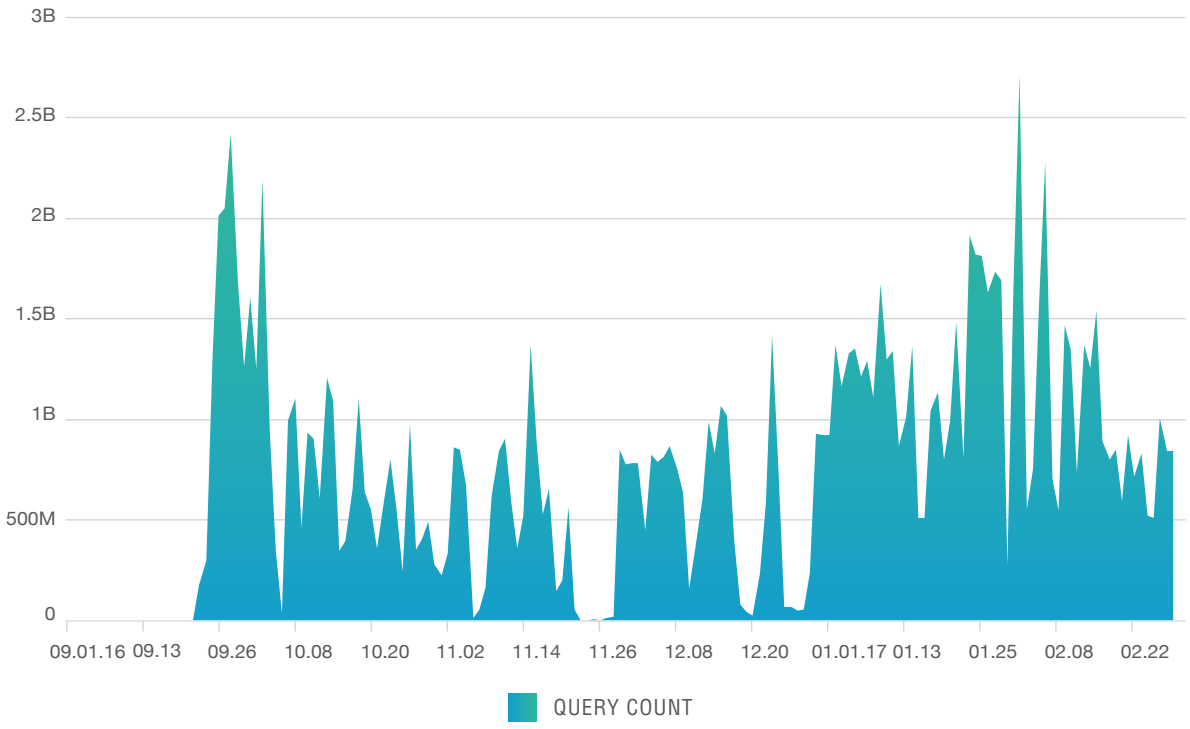
PRSDs

In the **Fall 2016 Data Revelations Report**, we described the history of PRSD attacks. This DNS-based DDoS attack type, which threatens the DNS infrastructure, first surfaced in 2014 and has been going strong ever since (with a few periods of lower volumes).

In the six months since we released our last report, we've seen PRSD attacks active daily, with an average of 706 million queries per day. If we look further and break the past six months into two quarters (October – December 2016 and January – March 2017), we see a significant increase in the number of PRSDs. Notice the peak shown on **Chart 13** in late January/early February 2017. (As a side note, understanding peak traffic is important because networks need to be sized to handle wide ranges of peaks rather than an average volume day.)

While the average number of PRSD queries in the first period is 583 million per day, the average number of queries in the second period is 982 million per day. This represents an average growth of 68 percent in a matter of three months.

CHART 13: **NUMBER OF UNIQUE PRSD QUERIES SEEN BI-WEEKLY, SEPT 2016 TO FEBRUARY 2017**



High-Profile PRSD Targets

On top of the overall PRSD growth seen in the current analysis, we also identified a shift in the nature of some PRSD targets. In most of 2016, the targeted websites were small and often shady. In 2017, we've seen multiple top-tier brand names becoming the latest victims of PRSD (as a matter of fact, 20 of them are ranked among the top 1,000 most-visited websites list according to Alexa).[1]

At this time, it is not clear who is behind this; it is possible a malicious actor tries to scan these sites to find existing subdomains (in brute force fashion), then use this information for further hacks—subdomains can be used to increase the attack surface or find hosted non-public applications that are usually easier targets.

At the same time, this could be part of an "ethical hacking" penetration test, with the intention of informing these high-profile companies about vulnerabilities in their site (for a service fee). In either case, we believe it is our responsibility as good citizens of the net to monitor and inform the web community about this trend.

Below is a list of the top 20 targets for high-profile PRSDs:

booking.com	groupon.com
indeed.com	prezi.com
vimeo.com	hulu.com
quora.com	asana.com
buzzfeed.com	kickstarter.com
yelp.com	surveymonkey.com
battle.net	coursera.org
zendesk.com	glassdoor.com
shopify.com	uber.com
udemy.com	okta.com

[1] https://aws.amazon.com/alexa-top-sites/

The ROI on ransomware is the best compared to all other financial attacks; it is unfortunately still the fastest and most lucrative way of making money online today.

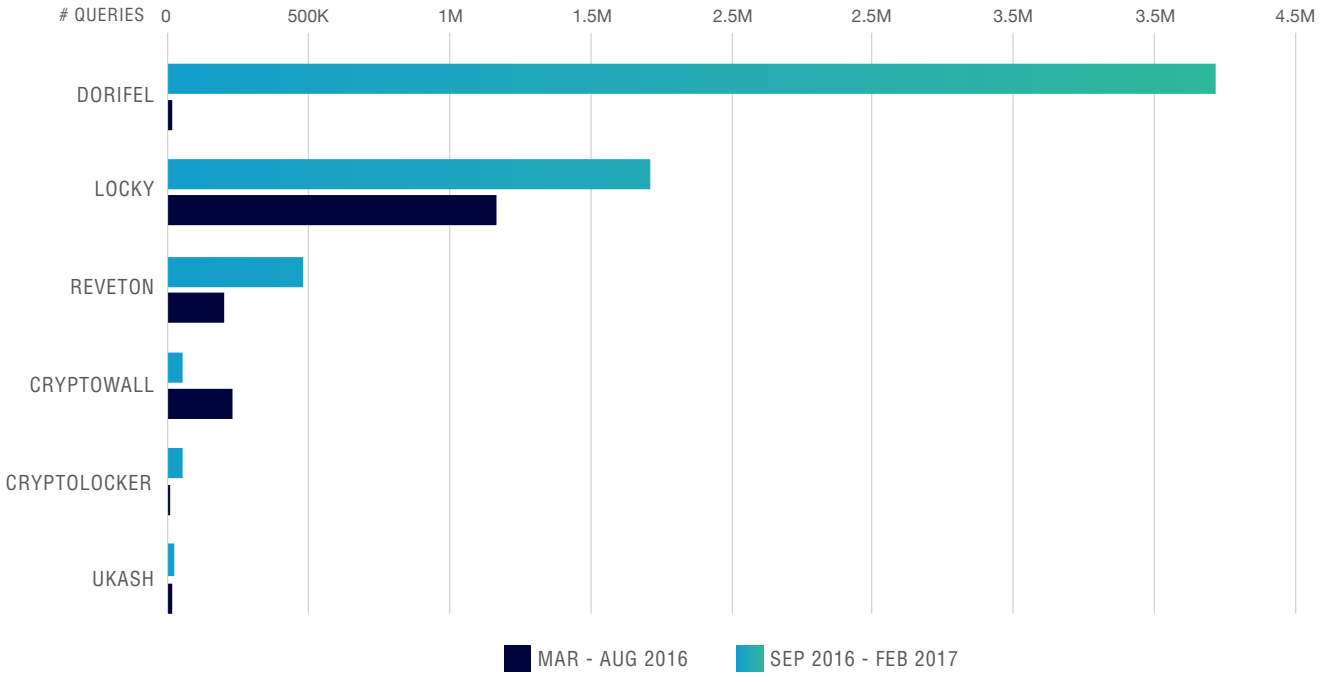
Ransomware Rising

The number of ransomware attacks has significantly increased since we last reported on it in October 2016. The pre-conditions and the financial incentive for this type of attack have remained the same: the ROI on ransomware is the best compared to all other financial attacks; it is, unfortunately, still the fastest and most lucrative way of making money online today.

Because people and businesses cherish their data, they are often willing to surrender to the ransom demand. Bitcoin makes the ransom payment transaction secure and private, so the chances of being caught by law enforcement are slim. And the more successful ransomware is, the more attackers are likely to join the "crypto rush."

The rise of Ransomware-as-a-Service has helped propel growth. Using this model, malware code authors offer ransomware services to anyone willing to pay the entry fee—no coding skills required—which is often less than $100.[2] These code authors take a cut of the proceeds while their malicious code spreads like wildfire.

CHART 14: **RANSOMWARE ATTACK QUERIES FROM MARCH 2016 TO FEBRUARY 2017**



[2] http://www.csoonline.com/article/3146537/security/ransomware-as-a-service-fuels-explosive-growth.html

The ransom itself has increased as well. In 2015, the average ransom was $294. By 2016, that number jumped to $679.[3] We expect to see that number grow further in 2017.

In the data we analyzed for this report, we've seen a significant increase in ransomware in general, with outbreaks of specific ransomware strains.

Overall, the number of ransomware queries increased by 270 percent between Fall 2016 and Spring 2017, with the majority of growth seen in the Dorifel ransomware activity.

Why Cybercrime is Not Prosecuted

While there are a handful of cases where ransomware creators were arrested, most cybercriminals enjoy a risk-free work environment. There are two main reasons for this:

1. Attribution: Who is responsible for arresting a Russian hacker who uses Necurs bots located in Brazil and Germany, to propagate spam emails with a financial Trojan that targets U.S. financial institutions? As explained in this report, the cyberattack ladder is a long, involved process. Determining which government entity and which country should pursue cyberattackers is difficult.

2. Cooperation: In the above example, even if governments and agencies are willing to investigate and have the time and money, the investigation requires collaboration between at least three countries, with multiple agencies involved in each country. If agencies cooperate and no agency breaks the process, it is very difficult to follow the money trail when Bitcoin transactions are almost completely untraceable.

[3] https://blogs.systweak.com/2016/08/ransomware-statistics-growth-of-ransomware-in-2016/

SPECIAL REPORT:

CYBERSECURITY AND SMALL BUSINESSES

50% of all SMBs are attacked at least once by cybercrime yet 77% of owners think they're safe from cyberthreats

60% of SMBs that are victims of cybercrime go out of business

Since 2013, the average cost of an attack on SMBs has skyrocketed from $8,699 to $20,752 per attack

While media outlets often focus on corporate enterprise breaches, small and mid-sized businesses are a primary target for cybercriminals. One reason cybercriminals target SMBs is that they are often underprepared for attacks and over-confident in their preparedness. Though a staggering 50 percent of all SMBs have recently reported cyberthreat activity[4], over 77 percent of them think they are safe.[5] Since reality often has a way of reasserting itself, the statistics help tell the story of how successful cybercriminals have been against unsuspecting SMBs.

Ransomware Attacks are a Hefty Price to Pay

One of the most successful attacks against small business is ransomware, often orchestrated by the Necurs botnet. In 2013, cyberattacks cost SMBs on average $8,699 per attack; today, attacks cost small businesses on average $20,752 per attack, according to a tutorial by Small Business Innovation Research and Small Business Technology Transfer (SBIR/SBTT).[6] The FBI reports that ransomware attacks cost victims nearly 10 times more in the first three months of 2016 than they did in all of 2015.[7]

SBIR/SBTT noted statistics from the National Small Business Association (NSBA) stating that over 68 percent of SMBs have been attacked more than once, but of those attacked (50 percent of the grand total of SMBs) 60 percent went out of business.[8] It is clear that the economic impact of cybercrime is severe, but a public statement released by the U.S. Securities and Exchange Commission (SEC) notes a more discouraging fact: SMBs that have become a victim of cybercrime are likely to be targeted again.[9]

New Attack Vectors Complicate Threat Landscape

Since many SMBs have business relationships with larger organizations, as pointed out by the SEC report, "cybercriminals are focusing on SMBs as a gateway into larger organizations, since SMBs' cyber defenses are typically less robust than those of larger organizations." Essentially, they are being used as a "test market" for threats with greater impact, and potentially greater devastation. The simple fact that SMBs are easier targets for cybercriminals, rather than larger scale organizations that have more cybersecurity resources, motivates criminals to launch a range of different attacks beyond ransomware which make threats more difficult to detect and stop.

The advent of IoT-based cyberthreats has rendered unsuspecting devices particularly vulnerable to attack, such as network printers and scanners, which can be used by botnets to commit large-scale DDoS attacks. Weak security increases the effectiveness of DDoS attacks when networks fail, completely inhibiting a business from operating. The result is substantial costs to businesses for every minute they cannot repair network functionality.

The growing trend of mobile and BYOD devices further complicates the cybersecurity landscape. Employees are constantly bringing devices onto the business network, taking them off and bringing them back again, increasing the risk for ransomware attacks and data theft.

Reduced network visibility causes network vulnerability since administrators are unable to control when a device enters a network and what security capabilities the device has. With the advent of sophisticated malware phishing attacks which often lead to ransomware attacks, securing individual devices with endpoint solutions does not solve the issue since human error (e.g., clicking on a malicious, false advertisement) is the main cause of infection, and thus network vulnerability.

DNS-based Solutions are a Key Element of Network-wide Cybersecurity

DNS offers a high level of visibility into a major part of the internet, from which 91 percent of cybercriminals launch attacks. By integrating DNS information into a multifaceted security architecture, organizations can gain visibility into parts of the internet that have been relatively obscure until now.

In Q1 2016, cyberattacks cost $209M, up nearly 10x from all of 2015 ($24M)

49% of attacks on SMBs are phishing attacks, which often lead to ransomware [10]

Ransomware-related losses by U.S. SMBs total more than $75B every year [11]

[4] http://www.cio.com/article/2908864/security0/5-costly-consequences-of-smb-cybercrime.html
[5, 6, 8] https://www.sbir.gov/tutorials/cyber-security/tutorial-1
[7] http://www.reuters.com/article/us-usa-cyber-ransomware-idUSKCN0X917X
[9] https://www.sec.gov/news/statement/cybersecurity-challenges-for-small-midsize-businesses.html#_edn7
[10] http://www.techradar.com/news/world-of-tech/management/small-businesses-face-big-risks-from-cybercrime-1323265
[11] http://gazette.com/easy-prey-5-startling-ransomware-stats-for-small-biz-owners/article/1595123

SUMMARY

Security Never Sleeps

It's been only six months since the **Fall 2016 Data Revelations Report**, but here's what we learned:

Six months in cybersecurity is like six years in any other field.

Change is a constant, and it is rapid. The more successful cyberattacks are, the more they drive additional attackers into the cybercrime ecosystem. With growth in the number of active players comes growth in the cyber activity seen through the DNS layer.

In this report, we broke cyberattacks into stages or rungs and showed findings and trends identified by Nominum Data Science. One of our key takeaways is, unsurprisingly, that DNS security is virtually anywhere. DNS is ubiquitous, and is therefore tied to almost every step of the cyberattack ladder. You can use DNS data to block malicious domains at the preparation stage, to curtail phishing at the intrusion stage or to block malware C&C communications in the attack stage. In specific attacks, such as ransomware, you can even obstruct the cybercriminal's monetary transactions.

You can use DNS data to block malicious domains at the preparation stage, curtail phishing at the intrusion stage or to block malware C&C communications at the attack stage.

The changes we've observed in the numbers of malicious queries are significant. Compared to the same month a year ago, the number of queries has grown fourfold. The specific threats that saw the greatest growth are the ones related to some of the worst financial scams (such as Necurs).

Change is not only an issue of volumes, it's also about the sophistication of malware; the typical malware lifecycle is rather short, usually less than a year. The number of new families of malware, new strains of contemporary malware, or evil evolutions of existing malware are ever-growing. Attackers are competing against the security community. They therefore need to come up with always-new security evasion techniques but they also compete against each other. In this free market, whoever has the better innovation, the more effective techniques or the better ROI wins. As in any good free market, this competition drives constant change and improvement.

In the Fall 2016 Data Revelations Report we predicted an increase in ransomware crime and DDoS attacks generated by IoT device botnets. In the past six months, we've seen these predictions come true. Since the root reasons for these cybercrimes have not changed since last year, we can predict with high confidence that the trend will grow and evolve.

One of the trends of both Ransomware and DDoS is the increased use of outsourcing. Ransomware-as-a-Service (RaaS) and DDoS-as-a-Service (DDoSaaS) do not represent a new business model, yet they seem to be getting more traction in 2017. Cerber became the most popular ransomware of 2017 after adopting RaaS as its main business model. The Mirai strain's masters started offering DDoS services as the main way to generate money from their botnet of compromised IoT devices.

In a similar fashion to other "as-a-service" models, attackers rent a malicious software/service instead of purchasing or developing it. (We see different activities offered as-a-service in all of the attack ladder stages: malicious software rental, malicious software distribution, or attack execution). The "crime-as-a-service" model offers many savings. It eliminates the upfront cost of purchase, while still providing attackers with support and maintenance. (Yes, reputable CaaS vendors offer customer support.) It saves attackers time from handling annoying IT issues. Most importantly, it makes cybercrime more scalable and accessible. When you "pay-as-you-go" for ransomware or DDoS attacks, you can change your usage plan easily and with a short notice. This means you get the flexibility to switch attack targets, attack volume or attack country in an instant.

The result of all this is … more cybercrime, which is what we see in our data. One more way we can use the Cyberattack Ladder is to look at existing security solutions and how they address phases of an attack.

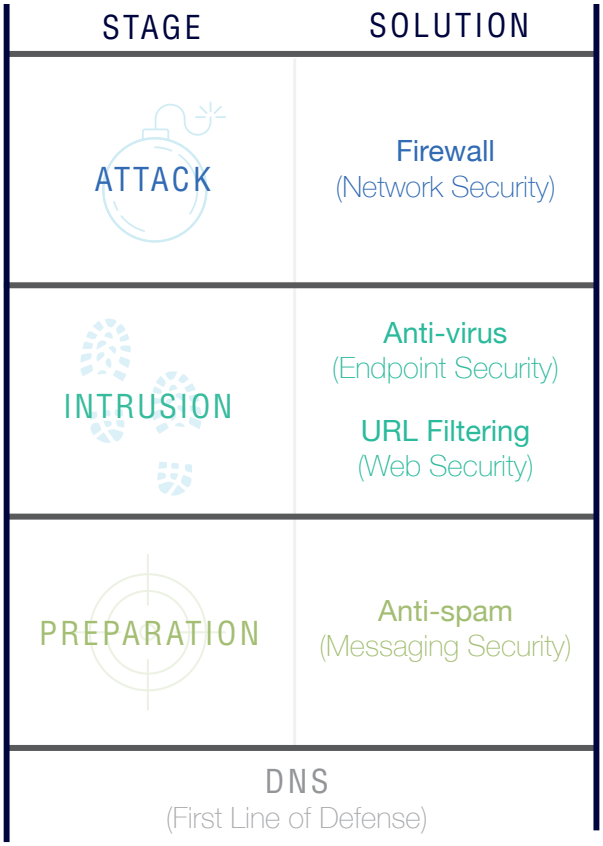


CHART 15:
CYBERATTACK SECURITY SOLUTIONS

When devising strategies to defeat crime-as-a-service, we recommend a multi-phased approach. Start with DNS for the first line of defense, and employ the other solutions listed in **Chart 15** as appropriate. As security practitioners, we believe that following the Cyberattack Ladder, understanding the attackers' perspective and understanding the methods attackers use (or exploit) is the first step in determining the countermeasures.

CYBERSECURITY GLOSSARY

General Malware Types

Malware

Shorthand for malicious software, malware is the umbrella term for software designed to disrupt or damage a computer system. For example, viruses and Trojans are two specific types of malicious software that serve different functions, but both are generally referred to as malware.

Trojan

A program that breaches the security of a computer system to erase, corrupt or remove data by tricking the user into opening it; a Trojan is unable to infect a computer if it is not opened by the user. The name derives from the infamous wooden horse constructed by the Greeks as a decoy, in which Greek soldiers hid to overtake the city of Troy.

Financial Trojan / Banker Trojan

A type of Trojan specifically designed to gain access to confidential banking information stored within a banking system by acting as legitimate software until it is opened by the user.

Virus

A type of malware program capable of self-replication which can interfere with or destroy other programs, and can transfer itself to other systems through disks or networks.

Computer Worm

Similar to a virus, a computer worm is a type of malware program capable of self-replication in order to spread onto other computers. To spread, worms rely on security vulnerabilities in a computer network. Worms usually cause damage, even if that just involves using bandwidth.

Malware by Purpose/Function

Rootkit

A concatenation of the words root and kit, the former being the traditional term for Unix-like operating systems, and the latter, which describes the software components that make up a tool. A rootkit is a collection of software tools used to gain root access to a computer without being detected.

Exploit Kit / Exploit Pack

An exploit kit is a software kit used to identify and take advantage of system/device vulnerabilities in order to distribute malicious software, such as financial malware.

Spyware

Spyware is used to secretly gather sensitive information about an individual or organization, and without knowledge or consent from the victim, transfer that data to a third party. Spyware comes in the form of either a Trojan, virus or worm.

Adware

Software that displays ads, generally in a user's web browser, that are unwanted and potentially contain malware. Adware is used for malicious purposes (i.e., to deliver a Trojan or virus), and also for tracking a user's browsing behavior to inform targeted advertising campaigns.

Ransomware

Prevalent and highly successful malware that holds an entire computer system or specific computer files hostage until a ransom demand is paid. Ransomware is delivered by other forms of malware, such as a Trojan or phishing email, tricking the victim to download the virus. Once the virus is loaded, it encrypts the system or certain files and demands a ransom payment (usually via Bitcoin or other cryptocurrency) to obtain the encryption key.

Keylogger / Keystroke Logging

Software often used in association with spyware and adware designed to covertly record a user's key strokes. This information can be analyzed and sent to third parties without the knowledge or consent of the user.

RAT

An acronym for Remote Access Tool, this software provides remote access to a computer. Although there are legitimate remote access tools on the market, the term "RAT" is mostly used for remote access malware, which is often the payload of a Trojan.

Backdoor

Term used for gaining remote access to a computer by circumventing standard/legal authentication methods.

Other Terms

Bot / Zombie

A computer that has been infected with malware designed to act in coordination with other infected computers around the world. Often, a bot is used for activities such as distributed denial-of-service (DDoS) attacks on a network, brute force attacks on login pages or bitcoin mining schemes.

Botnet

A group of bots infected with the same malware for the purpose of launching a coordinated attack on a desired online target.

Command and Control Server (C&C)

Often, malware will "phone home" or connect to a hacker-developed server to either receive instructions, upload stolen data or both. The hacker-developed server is essentially the headquarters of the attack, referred to as a command-and-control (C&C) server.

Dropper

A script or program responsible for carrying, running and installing malware onto the targeted system. Droppers do not cause harm themselves but can deliver the payload without detection.

Exploit

Malicious software or a piece of malicious code that is used to take advantage of a computer vulnerability in order to cause harm to, gain control of or take down the system or network.

In the Wild

Malware that has gone past the development environment and is considered post-release, actively being distributed on or between unsuspecting users across the internet.

Payload

The software installed by a dropper is referred to as the payload. The payload is the part of the malware that does whatever job the malware is intended to do.

Variant

Most malware does not remain static but changes over time. Different versions of a particular malware program are referred to as variants. A variant may include minor changes that help the new variant slip past anti-virus software.

Vulnerability

A weakness in a piece of software: a system, an application, a plug-in or anything else. This weakness allows an attacker to gain unauthorized access to a computer at which point it installs malware. The software that actually takes advantage of the vulnerability is called an exploit.

Zero-day

Zero-day is a term that refers to a hole in a software program that its developer does not know about. When a cybercriminal takes advantage of this vulnerability, the developer suddenly becomes aware and scrambles to fix it. Zero-day attacks are particularly dangerous because they can easily bypass all defense protocols, including anti-virus and other endpoint solutions.

About Nominum

Nominum™ is a pioneer and global leader in DNS-based security and services innovation. The Silicon Valley company provides an integrated suite of DNS-based applications that enable fixed and mobile operators to enhance, secure and personalize the online subscriber experience. Nominum N2™ solutions leverage the company's market-leading Vantio™ unified DNS platform and an expert team of data scientists to provide closed loop security solutions, which include: protection of fixed, mobile and converged networks from malicious attacks; security for online and mobile users from threats like phishing, ransomware and other malware; personalized customer alerts and remediation of infected devices. The result for operators is improved service agility, increased brand loyalty and a stronger competitive advantage.

More than 130 service providers in over 40 countries trust Nominum to deliver a safe, customizable internet and promote greater value to over half a billion subscribers. Nominum DNS software resolves 1.7 trillion queries around the globe every day—roughly 100 times more transactions than the combined daily volume of tweets, likes, and searches taking place on major web properties. For more information, please visit nominum.com.

Our Products

Vantio™ CacheServe

Network operators can provide a safe and reliable internet with the industry's highest-performing and most secure carrier-grade caching DNS server.

N2™ Big Data Connector

Allows service providers to easily integrate DNS data into their big data platform for better subscriber insights.

N2™ ThreatAvert

DNS-based, carrier-grade cybersecurity application that protects service provider networks and subscribers against ransomware, DDoS, phishing, malware, viruses, botnets and more.

N2™ Secure Business

Lets providers leverage their existing DNS investment to deliver a SECaaS solution that protects business customers from cyberthreats like phishing, ransomware and malware.

N2™ Secure Consumer

Cloud-based cybersecurity solution that protects subscribers and IoT devices from phishing, viruses, ransomware and malware.

N2™ Secure Public Wi-Fi

Lets providers leverage their existing DNS investment to deliver a SECaaS solution that shields Wi-Fi guests from inappropriate and unsafe content.

N2™ Reach

Deliver timely, personalized in-browser messages through a carrier-grade platform and convert at 5 to 15 times higher rates than email.

Vantio™ AuthServe

Authoritative DNS offers subscribers a carrier-grade solution for better user experience while reducing operating costs with exceptional ease of use, scaling and stability.

800 Bridge Parkway, Suite 100 Redwood City, CA 94065 | +1 (650) 381-6000 | **hello@nominum.com**