DATA REVELATIONS

Nominum Data Science Security Report

nominum™

Fall 2016

EXECUTIVE SUMMARY

October 21, 2016 was a day many security professionals will remember. Internet users around the world couldn't access their favorite sites like Twitter, Paypal, The New York Times, Box, Netflix and Spotify, to name a few. The culprit: a massive DDoS attack against a managed Domain Name System (DNS) provider not well-known outside technology circles. We were quickly reminded how critical the DNS is to the internet as well as its vulnerability. Many theorize that this attack was merely a Proof of Concept, with far bigger attacks to come.

The DNS is often misused by cybercriminals for their attacks. 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. Nominum Data Science analyzes over 100 billion DNS queries per day from live DNS query streams around the world to detect emerging threats before they become publicly visible.

Nominum is pleased to share the unique insights from this team as part of our inaugural Security Report **Data Revelations: Fall 2016**. Not surprisingly, the report shows that profit-motivated attackers are often outpacing defenders as they continue to evolve their attacks to avoid countermeasures of the security community. The report investigates the largest threats that affect organizations and individuals, including ransomware, DDoS, mobile malware, IoT-based attacks and more.

Based on an analysis of 15 trillion DNS queries between March 1 and August 31 in 2016, the report also aims to provide a timely snapshot of the security landscape between the publishing windows of the semi-annual and mid-year reports from other security vendors.

Some key findings:

- Nominum sees over 5 million new domains queried daily, the vast majority of which are malicious yet unknown to security vendors.
- Pseudo Random Subdomain (PRSD) DDoS attacks have resumed and are now targeting popular domains.
- The majority of command and control infrastructure is hosted in the U.S.
- Botnet command and control activity jumped in August, driven by Necurs, the most wide-spread botnet family.
- The hard-to-remove Ghost Push Android malware dominates the mobile malware landscape.
- Since the Mirai botnet code release, the number of PRSD targets using Mirai has grown fivefold.
- The Mirai botnet is continuously executing DNS attacks, perhaps presaging another big attack.

We hope you find this report to be insightful. If you have questions about its content, please contact us at hello@nominum.com.

Sincerely,

Craig Sprosts, Vice President of Product & Strategy

Yuriy Yuzifovich, Head of Data Science & Security Research

CONTENTS

1 ON KNOWN UNKNOWNS

"As we know, there are known knowns; there are things we know we know.

We also know there are known unknowns; that is to say we know there are some things we do not know.

But there are also unknown unknowns – the ones we don't know we don't know. And it is the latter category that tend to be the difficult ones."

–DONALD RUMSFELD

INTRODUCTION

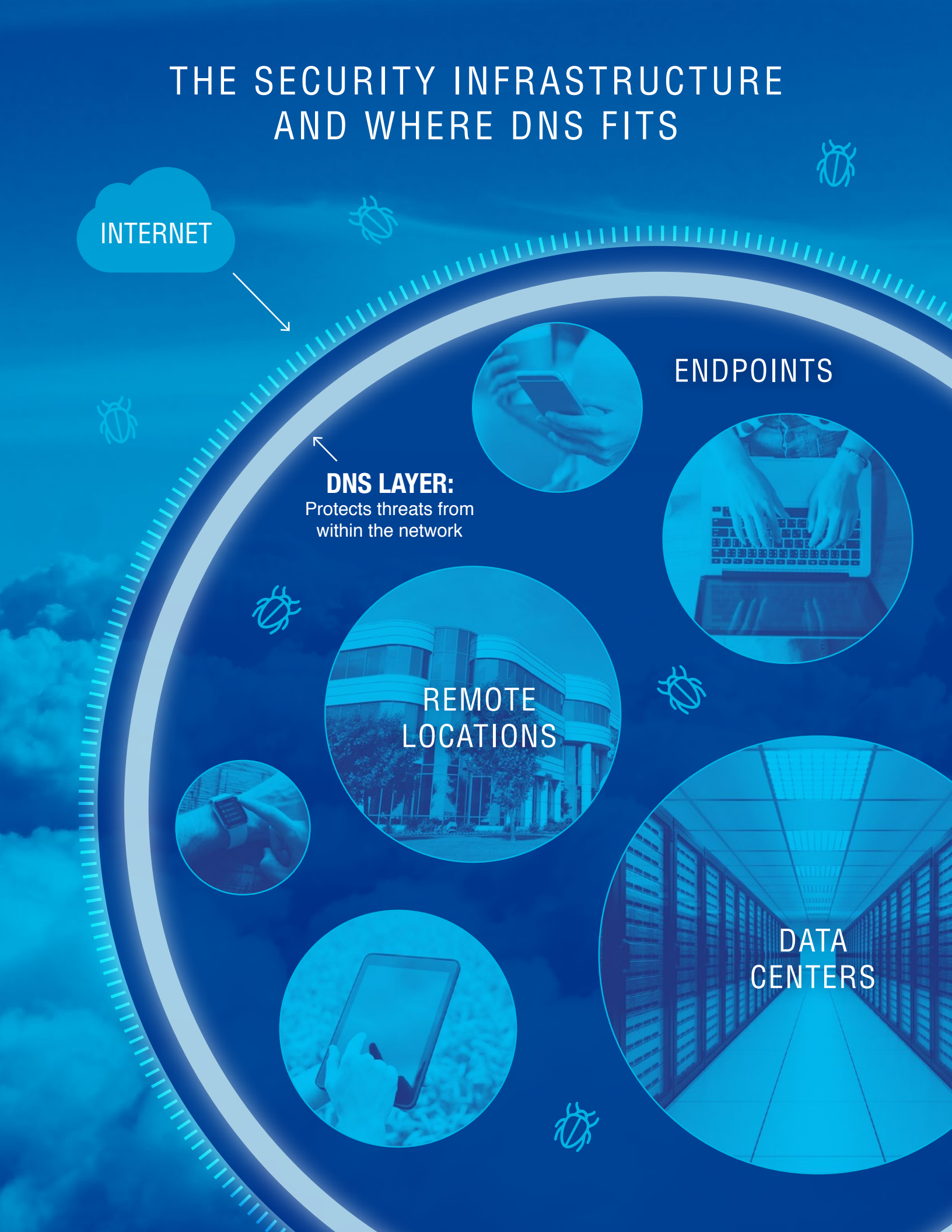
In February 2002, Defense Secretary Donald Rumsfeld started a Department of Defense briefing with a speech on the danger of unknown unknowns. Though the concept is often associated with Rumsfeld, it dates back to 1955 when American psychologists used it to describe the examination of the unconscious mind. When it comes to scientific inquiry, exploring known unknowns is where the bulk of time is spent, particularly in the arena of cybersecurity. Cybersecurity experts, like those on the Nominum™ Data Science team, spend their days and nights examining the footprints of cybercriminals to track anomalies, connect disparate dots and predict the next steps of highly sophisticated criminals who go to great lengths to disguise their exploits.

This inaugural edition of the Nominum Data Science Security Report comes from the frontlines of the war against cybercrime. On a daily basis, Nominum Data Science examines over 100 billion DNS queries from live DNS query streams, extracted from production DNS resolvers around the world. Machine learning techniques are applied to the data and the results are combined with other data sources to find and validate new threats from across the globe. These attacks threaten Nominum's customer base of Communications Service Provider (CSP) networks and subscribers.

This report breaks down the cyberthreat landscape as it relates to DNS. DNS, often thought of as the phone book of the internet, associates names (e.g., Nominum.com) with an IP address. Because of its ubiquity (virtually all internet lookups depend on it) DNS offers an ideal platform for cybercriminals to launch and manage a wide range of exploits. In fact, 91.3 percent of malware uses DNS.[1] Thus, thorough examination of DNS data provides unique insight into the patterns and techniques of cybercriminals.

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

THE SECURITY INFRASTRUCTURE AND WHERE DNS FITS



DNS and security

DNS security has two distinct meanings. First, DNS is mission-critical infrastructure that all organizations rely on and cannot function without. Yet DNS remains a vulnerable component in the network that is frequently exploited as a launch platform for cyberattacks and is inadequately protected by traditional security solutions. When critical DNS services are compromised, it can result in catastrophic network and system failures. Hence, DNS security is applied to protect DNS servers.

Second, DNS plays a critical role in the present-day layered security design known as "defense in depth," where no single solution addresses all exploits, which means multiple approaches to cyberdefense are needed. In today's threat environment, where organizations and individuals are being targeted, using traditional security layers in silos (cloud, network, data and endpoint protection solutions) does not provide adequate protection. Attackers are knowledgeable about how each layer works. Therefore, they know how to bypass each individual layer. Gathering independent information from multiple distinct sources and then sharing that information between the different layers is the key for blocking today's attacks.

By integrating DNS information into a smart security architecture, organizations can get visibility into areas of cyberspace that have been relatively obscure until now. Correlating DNS security events with events happening elsewhere in the infrastructure (endpoint, email, network, etc.) greatly improves threat detection and prevention chances.

This report looks at today's threat landscape, including DDoS, amplification and random subdomain attacks. We examine emerging and pervasive threats, such as Locky ransomware, and dive deep into the shifting and expanding security perimeter, including new threats introduced by IoT, BYOD and more. Finally, we look forward to 2017 and make predictions about coming shifts in the cyberthreat landscape.

We can't predict the unknown unknowns, but this report highlights the systems, techniques and responsiveness of Nominum Data Science that enable swift detection of threats as they become known unknowns.

Why DNS?

The process of internet name resolution maps application requests and domain names with IP addresses making the internet more "human" and navigable by any natural language. This may sound like a simple process but the Domain Name System (DNS) is positioned at a unique network point, holding the key to valuable information.

2 LEARNING FROM YESTERDAY

"Learn from yesterday, live for today, hope for tomorrow. The important thing is not to stop questioning."

-ALBERT EINSTEIN

SUMMARY OF TODAY'S LANDSCAPE

Businesses have long experienced the catastrophic damage a single cyberattack can cause. When a network is attacked, an organization's traffic is impacted and productivity slows to a crawl. Sensitive employee and company information may be compromised, which can impact the organization's brand and market value. For service providers, costly support calls escalate and long-term reputational damage ensues. In response, the cybersecurity philosophy has evolved from being reactive to proactive. The goal is to implement predictive intelligence to stop attacks before they wreak havoc, thereby protecting financial and human resources needed to resolve an attack.

In order to provide proactive protection, Nominum Data Science analyzes daily, weekly and quarterly data to predict the next steps cybercriminals will take. A relatively quiet period such as a diminishment in DDoS attacks does not necessarily mean that a certain threat has been resolved, or that all is well with the network. We know that cybercrime is too lucrative to simply fall off the map. We must understand the great lengths cybercriminals will take to disguise their footprints. Therefore, this silence leads us to question more, rather than less, to search for faint signals that could indicate an impending attack.

Methodology

While this is the first report of its kind from Nominum, data analysis is the lifeblood of Nominum Data Science. This report is a culmination of several months of analysis as detailed below. This sample represents approximately three percent of total global traffic.

Data

Metric	Value
Analysis time frame	3/1/2016 – 8/31/2016
Total query volume	14.7 Trillion
Average # of unique domain names per day	422.9 Million

Tools and outputs

The science of detecting threats using DNS data employs a variety of proprietary data analytics tools and algorithms:

- **Anomaly detection engine**: Identifies anomalies in the data by comparing each queried domain to previous domain behaviors, or by identifying newly generated domains.
- **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.
- **Correlation engine**: Identifies subtle relationships between domain names and the clients that query them. This tool is specifically used to detect and cluster families of malicious domains.

Taking the temperature

In order to gauge the overall threat level for a period, the Nominum Data Science team analyzed the relationship between malicious domains, infected clients and the queries made to these domains, using an extensive set of data. This approach produces a big picture view and helps to identify where the main threat lurks and where the next innovation is needed. This is not "perceived risk," but the actual risk as told (or measured) through big data analysis.

The trend seen by Nominum Data Science over the past six months has been clear and consistent. Starting around mid-year 2016, the rate of malicious traffic has tripled. Since a high percentage of malicious queries are made to Command and Control (C&C) servers, there has also been a formidable increase in the number of malicious domain names. These malicious domain names are frequently used as botnet communication and control points.

A deeper investigation of these results reveals high botnet activity during the last period, specifically from Necurs—the largest botnet existing today. More about that later in this report.

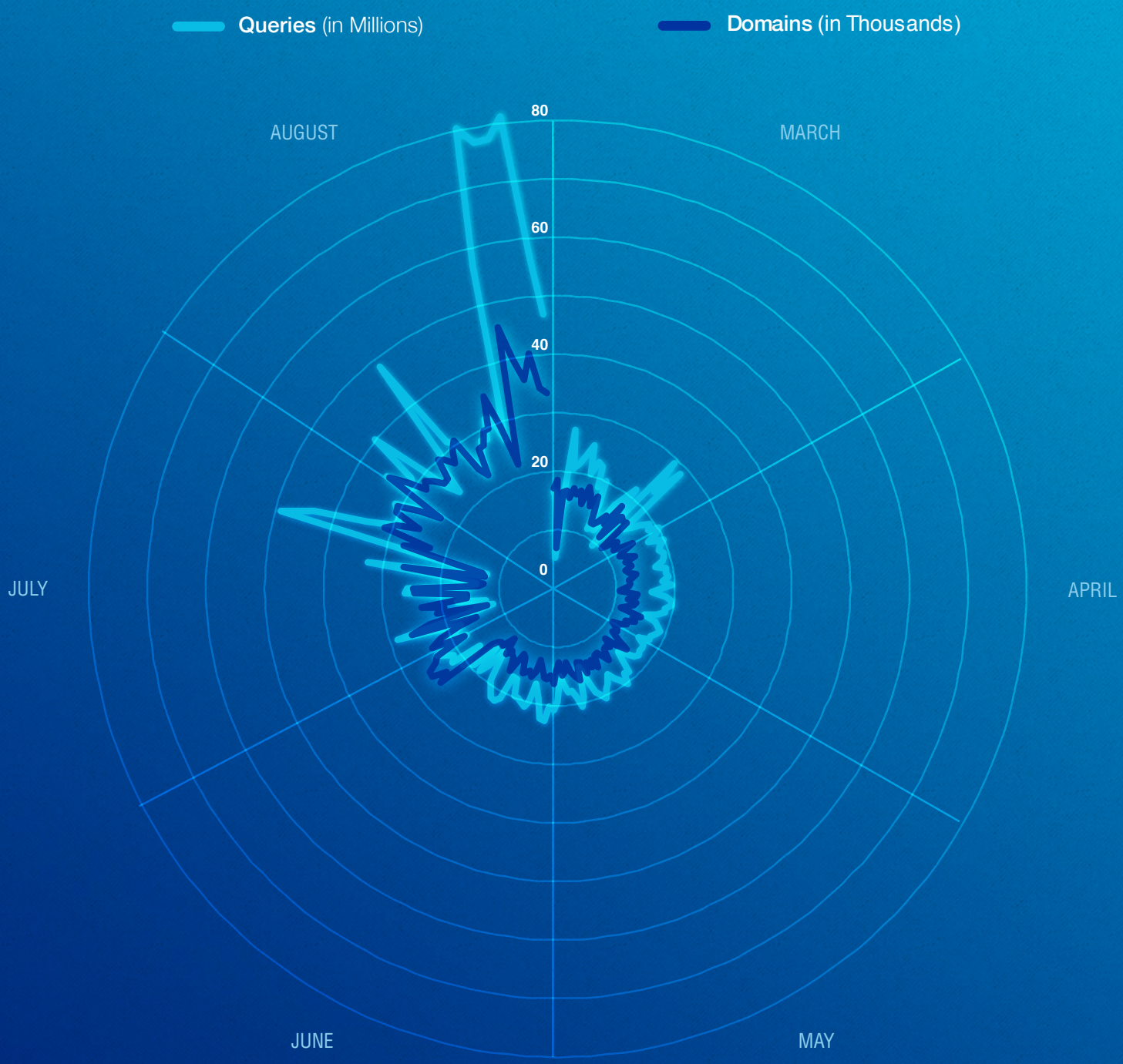
That's no barbershop domain

The DNS layer provides excellent visibility into new domains—defined as domains that are seen for the first time in DNS queries. Nominum Data Science tracks new domains hourly, regularly examining how many are generated each month.

The security-related significance of new domains comes from understanding the reason new domains are created. Approximately five million new domain names surface every day. We don't assume five million new people or companies have decided to open their own shop online each day. Rather, we see many of them as new domains that are generated by machines—specifically via Domain Generation Algorithms (DGAs)—that are purpose-built to serve as C&C servers for malware. Rarely are such domains created for a new barbershop.

The statistics for known vs. less-known (or suspicious) new domains are surprising. By analyzing the number of domains generated each month and the number of queries against those domains, Nominum Data Science can gauge how many domains are generated with malicious intent. As shown, 75 percent of all domains for the six-month period had only a single query against them. A few of them are accidental typos, but the majority are likely to be created with malicious intent—either to take an active part in cybercrime, or deceive security organizations fighting cybercrime (the probability that a domain such as "3isgarauile.tk" is a typo is quite small). This demonstrates one of the unique qualities of DNS compared to other network security methods. With as little as a single transaction, it can tell with high confidence that something malicious

THREAT TRACKER 2016



GROWTH IN QUERIES & DOMAINS

3X

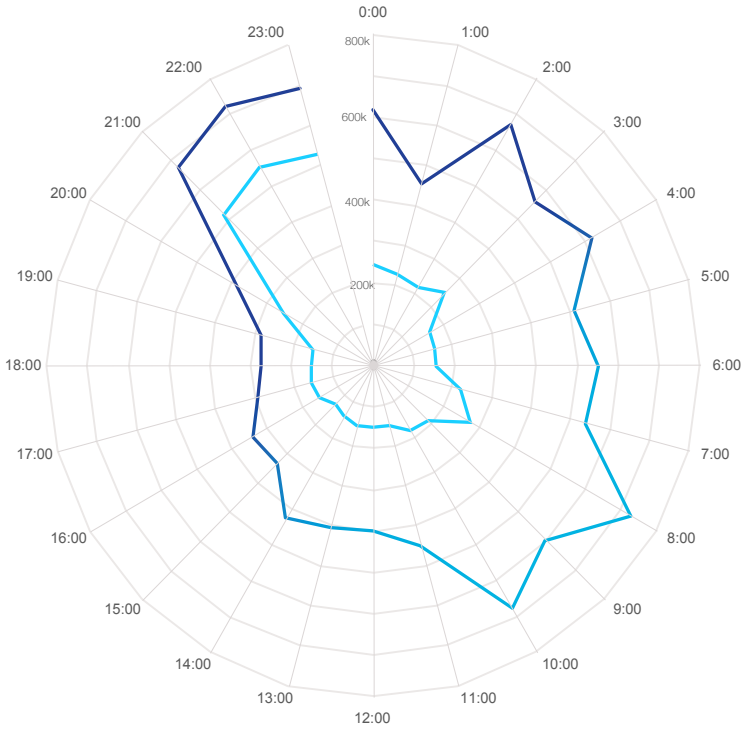
MALICIOUS QUERIES DAILY BY END OF AUGUST

82 million

DOMAINS ADDED DAILY TO BLOCK LIST

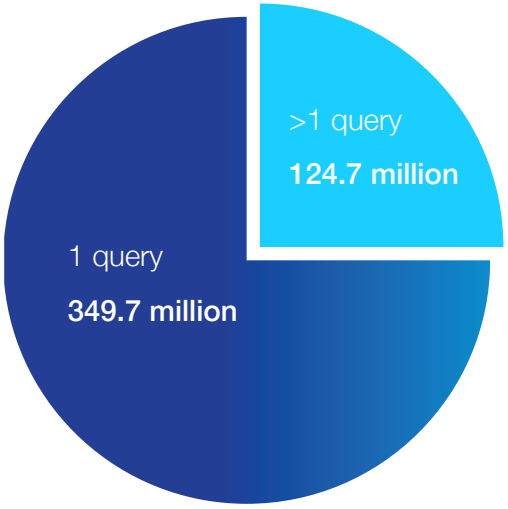
94,000

New domains over a 24 hour period



75% of domains had only 1 query*

*over 6-month period



NEW DOMAINS PER DAY

5 million

NEW DOMAINS PER MONTH

150 million

NEW DOMAINS MARCH – AUG 2016

1 billion

is happening. The other 25 percent of new domains that have more than a single query are also mostly malicious. Here our algorithm can connect unrelated new domains into clusters, with a high level of confidence.

Since these domains are likely malicious, top providers trust Nominum to block access to such domains until they are verified as legitimate. On average, Nominum blocks nearly 100 million queries daily. Doing so provides a sound security measure to avoid exposing provider networks to 'unknown' threats.

The Nominum 2016 Razzie Awards for Cybercrime

The Golden Raspberry Awards, or Razzies, is a ceremony that recognizes the worst Hollywood films of the year, hosted the day before the Academy Awards. Nominum has developed its own Razzie Awards to showcase the worst in cyberthreats—those persistent and popular threats that have appeared in the threat landscape so far in 2016.

Botnet award: **Necurs**

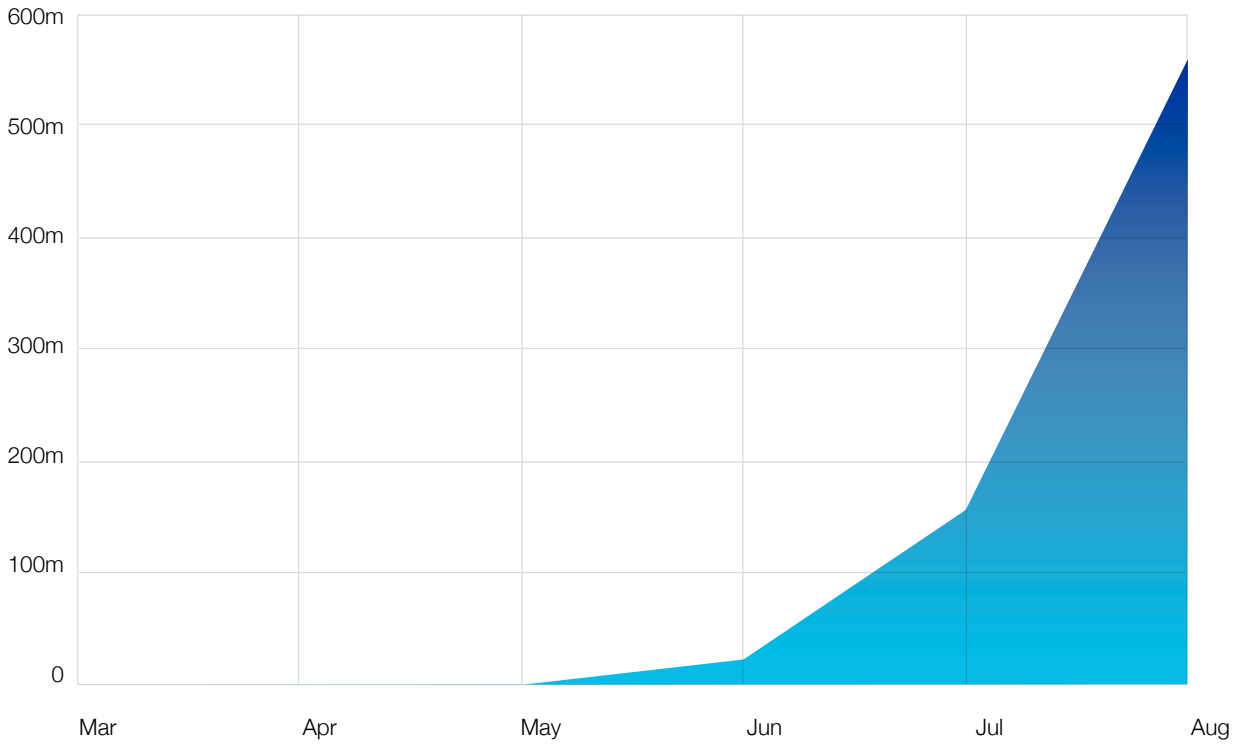
A botnet is a number of internet-connected computers communicating with other similar machines. Components located on networked computers communicate and coordinate their actions by C&Cs or by passing messages to one another.

The Necurs botnet is one of the world's largest botnets with more than six million related machines under cybercriminal control. It is run by Russian organized cybercrime[2] and is responsible for millions of dollars in losses tied to the Dridex banking Trojan and more recently, the Locky ransomware strain.

Necurs exploded onto the scene in June 2016, a few months after we first started monitoring its C&C servers. The number of Necurs-related queries reached 558 million in August 2016. As many as 59 million queries have occurred on a daily basis. Necurs also has at least 10,000 live domains on any given day. Some of these are used as C&C servers, while the rest are used as decoys to deceive security experts.

Runner up—Mirai: Mirai botnet activity dramatically increased just after the measurement period for this report when the malware author(s) released the source code publicly on September 30. In most cases, the bots are DVRs, routers and IP cameras. Malware authors often use default manufacturer passwords, which most users never change, in order to commandeer the devices. Prior to the code release, we identified a few PRSD attacks against three targets, utilizing over 50,000 Mirai bots. Since the release, the number of targets has grown five to six times and Nominum estimates the number of bots involved has also significantly increased.

CHART 1. **NECURS QUERIES BY MONTH**



[2] Source: https://blog.knowbe4.com/what-is-the-necurs-botnet-and-how-does-it-spread-locky-ransomware

CHART 2. **NUMBER OF QUERIES TO THE NECURS BOTNET BROKEN DOWN BI-WEEKLY**

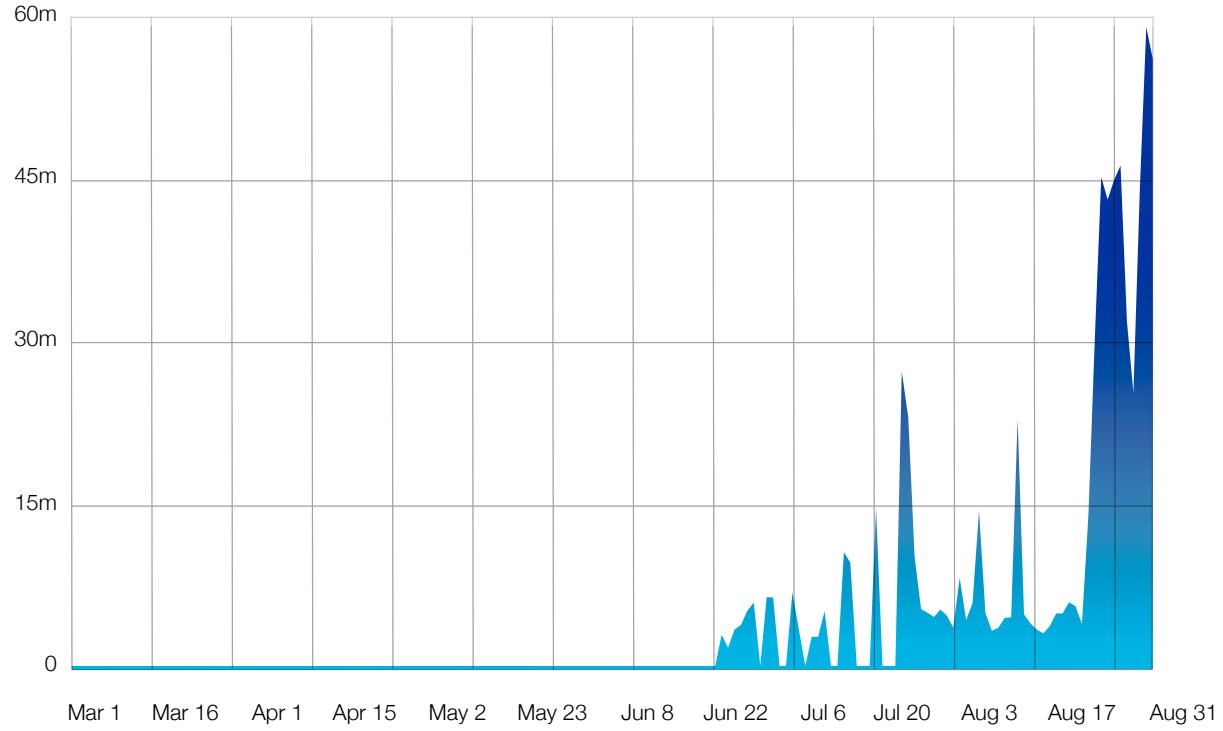
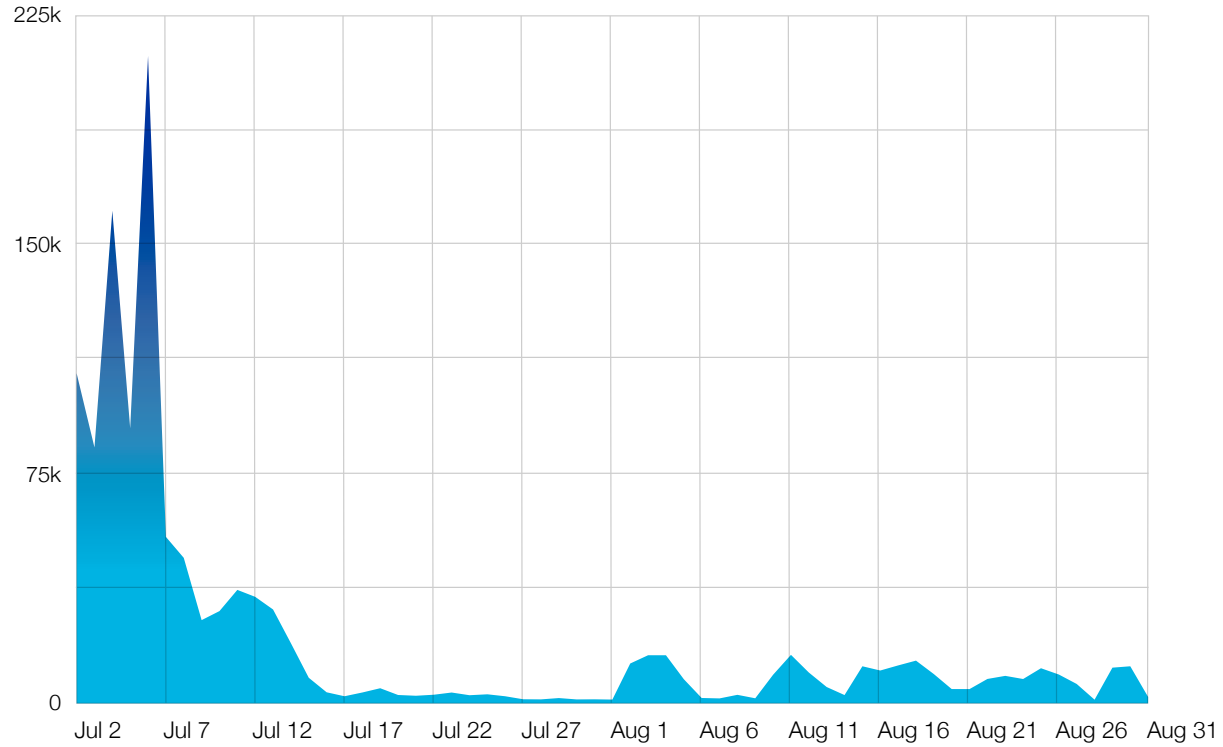


CHART 3. **NUMBER OF LOCKY QUERIES BROKEN DOWN BY WEEK**



Ransomware/financial Trojan award: **Locky**

The Locky ransomware strain came into the limelight for its $17,000 payday when it encrypted and held for ransom data from more than 250 computers at the Hollywood Presbyterian Medical Center in February 2016. It quickly became the most popular ransomware of 2016,[3] both in terms of the sheer number of infections and money generated from owners of the infected devices.

The heyday for Locky came in early July when a huge number of clients became infected with Locky and began communicating with their C&C servers.

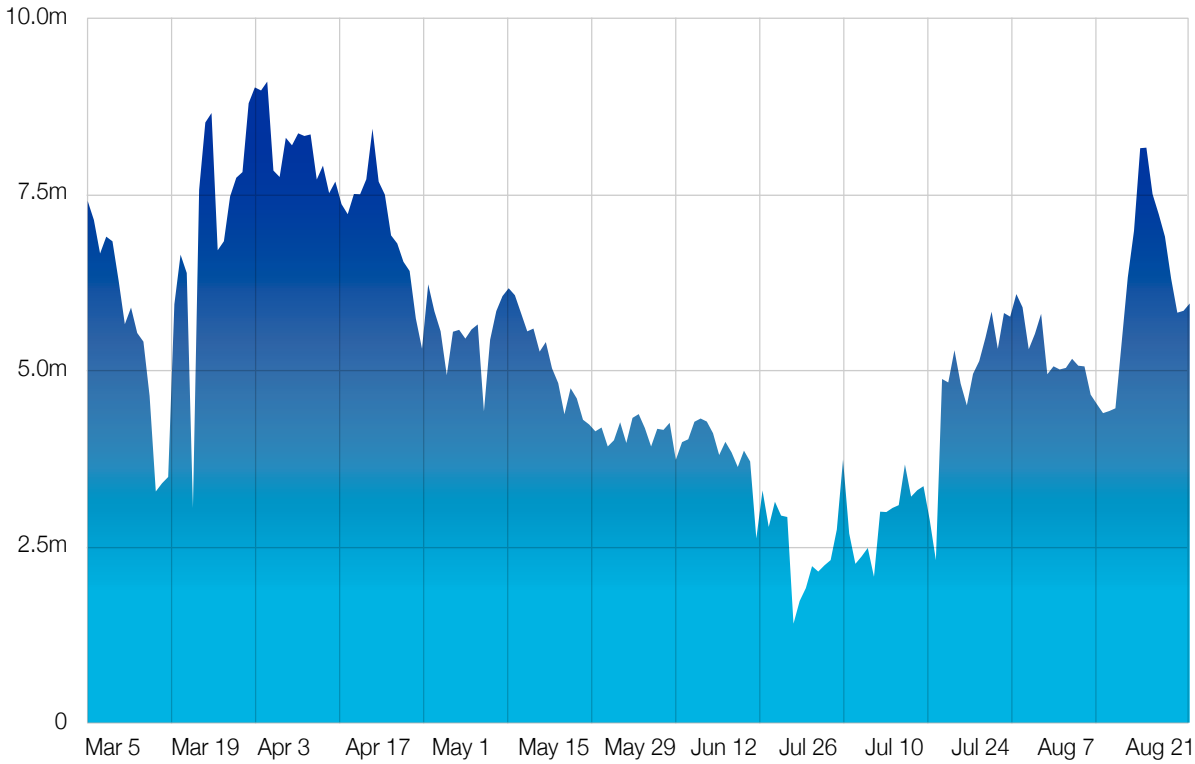
Runner up—CryptXXX: This popular ransomware has been hitting the net since April 2016.[4] When victims are infected, they will have their files encrypted and a ransom of about 2.4 bitcoins (approximately $1,000 USD) is required to receive the decryption key.

Runner up—Cerber: This ransomware has been offered as a service on a closed underground Russian forum since early 2016. Ransomware as a Service (RaaS) means that affiliates can distribute the ransomware, while the Cerber developers earn a commission from each ransom payment.

Fastest-growing malware award: **Ghost Push**

Ghost Push is malware that infects Android devices by automatically gaining root access, downloading malicious software (apps), converting it to a system app and then losing root access, which makes it virtually impossible to remove (even by factory reset, unless the firmware is re-flashed). The malware hogs all system resources, which drains the battery and makes the device unresponsive.

CHART 4. **GHOST PUSH QUERIES BROKEN DOWN BI-WEEKLY**



[3] http://www.forbes.com/sites/thomasbrewster/2016/02/18/ransomware-hollywood-payment-locky-menace/#1126ba0775b0

[4] https://sentinelone.com/item-news/cryptxxx-ransomware-racking-victims/

Ghost Push has been a clear and present danger throughout 2016, with over 100 million queries per month and over 110,000 infected devices seen daily in our data set. With the growth of malware dedicated to mobile devices, we expect the number of infected Ghost Push devices (and its copycats) to keep rising in the next year.

Runner up—Jadre: This Trojan has been quite active in the past six months. Our sample data showed consistent month-over-month growth in the number of DNS queries, with more than two million queries made in each of the past four months.

Runner up—Dorkbot: A device infected with Dorkbot malware (a different family of malware) will join the Dorkbot botnet. This botnet has seen increased activity this year distributing spam, taking part in DDoS attacks and harvesting users' credentials for online services, including banking services.

The whole world in their hands

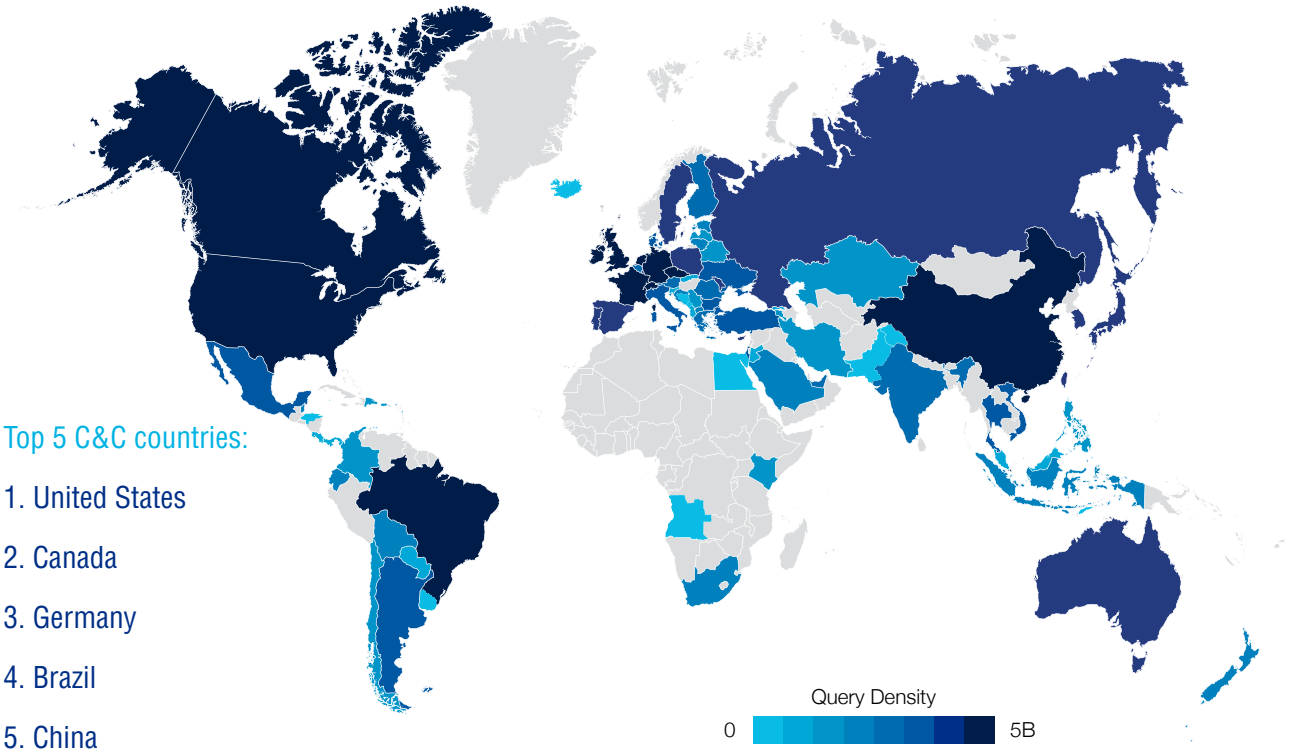
Cybercriminals take clever paths to disguise their exploits and operate within increasingly sophisticated, global networks. DNS data does not reveal where cybercriminals live, but it does reveal where C&C servers exist. These centralized computers issue commands to a botnet (typically infected devices) and are vital tools in a cybercriminal's tool kit.

Chart 5 presents the worldwide distribution of C&C servers over the past six months. More specifically, it shows the number of queries made to these servers by malicious actors (malware, bots, ransomware, etc.) and in which countries these servers are located. It is worth noting that many of these servers do not know they are part of cybercrime; they have either been compromised by hackers or paid for without revealing the malicious intent.

Looking at the map, it is clear that the U.S. is the top location of C&C servers. Nominum Data Science has witnessed nearly five billion DNS queries made to servers located in the U.S., which constitutes 46 percent of the total world activity. While this is obviously more than the U.S. percentage of the world's population, it is certainly aligned to its percentage of global IT spending. According to the 2014 IDC blackbook, the U.S. made up approximately 40 percent of global IT spending in 2013.

Once again, while this doesn't tell us where the bad guys are located, it does reveal which states have the most infrastructure under cybercriminal control. Cybercriminals (who may physically be located in other countries) benefit from using C&Cs in a location close to their victims. Given its population size and overall wealth, it is clear why the U.S. provides an inherent incentive for cybercriminals. Additionally, using servers in their home country can make it easier for local authorities to reach the cybercriminals and bring them to justice, so they obviously prefer to not do that.

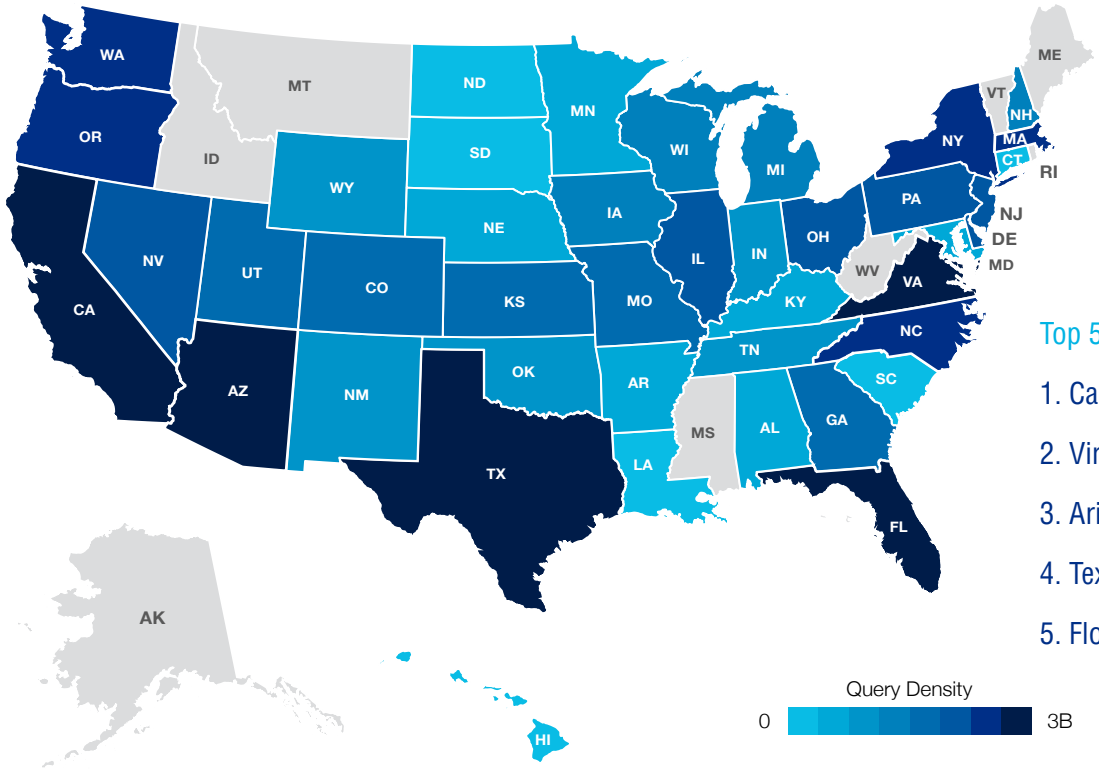
CHART 5. **TOP LOCATIONS OF MALICIOUS WEBSITES AND C&CS: GLOBAL**



Top 5 C&C countries:

1. United States
2. Canada
3. Germany
4. Brazil
5. China

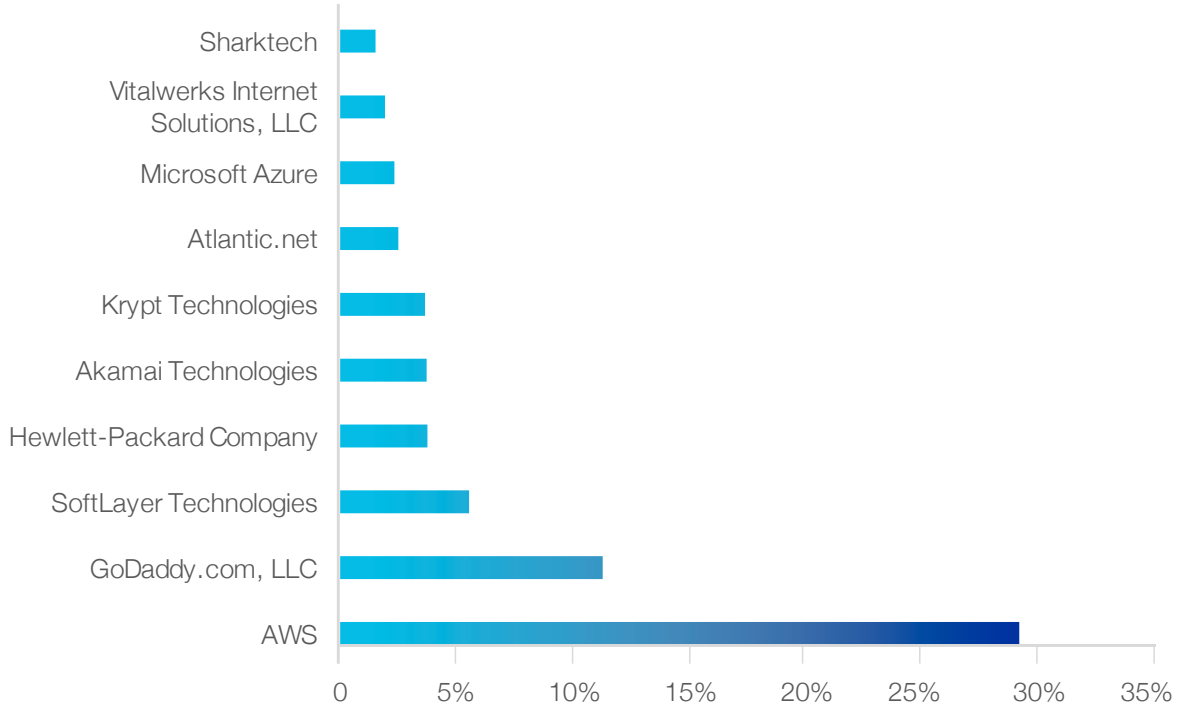
CHART 6. **TOP LOCATIONS OF MALICIOUS WEBSITES AND C&CS: US**



Top 5 C&C States:

1. California
2. Virgina
3. Arizona
4. Texas
5. Florida

CHART 7: **TOP 10 MALWARE HOSTING, U.S.**



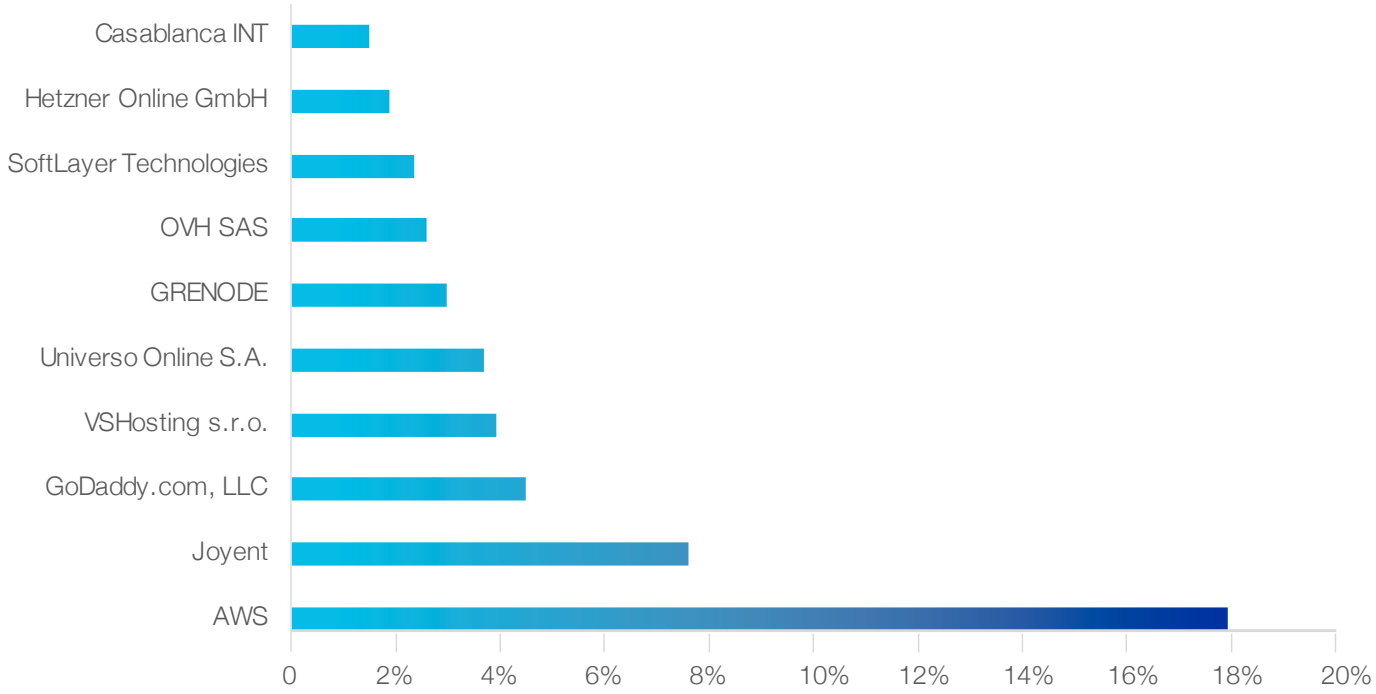
When it comes to web hosting, many organizations unknowingly host malicious servers; these servers reveal important information about the hosting tactics of cybercriminals.

One of the ways that malware activity on a network is spotted is via signals of their network activity. Cybercriminals are aware of that, and therefore look for ways to make things difficult for security organizations. One masquerade tactic is using a large number of domain names, and using each of them for short periods of time. Another way is using a geographically distributed operation as we saw in Charts 5 and 6.

The next 'deception' technique is hosting malware and C&C servers on cloud servers. To set up a malware host, a cybercriminal can opt to use an underground hosting service and operate their drop-site or C&C from there. While this is certainly an option that makes it harder for law enforcement and security companies to reach the host and take the site down, it also makes life easier for security organizations to classify a domain as malicious only by association with the known malicious hosting service.

The alternative is to abuse a hosting service that isn't obviously malicious. It may be taken down faster, but it will force security organizations to work harder to detect it. As seen in Charts 7 and 8, Amazon Web Services (AWS) is the most popular host for malicious sites, along with other big names (GoDaddy, HP, Microsoft and others).

CHART 8: **TOP 10 MALWARE HOSTING, WORLDWIDE**



Spotlight: DGAs

DGAs are a "must-have" item in any cybercriminal's tool kit. They create domains that are used by botnets to communicate to their C&C server. By some estimates, DGAs can generate up to 50,000 domains in a single day. Most cybercriminals use domain fluxing to disguise their activities; by constantly changing the domain of a C&C, an infected device (or botnet) can stay in operation longer.

3 EXPLOITERS & THE EXPLOITED

"When knowledge is limited - it leads to folly...

When knowledge exceeds a certain limit, it leads to exploitation."

-ABU BAKR

RANSOMWARE, DDOS AND AMPLIFICATION

One of the biggest changes witnessed in the cyberthreat landscape is the increasingly agile nature of malware. While older threats such as DDoS and amplification attacks continue, emerging and highly sophisticated threats such as Locky ransomware are wreaking havoc on individuals and businesses. This chapter examines these threats and provides commentary on aversion techniques.

When lightning strikes: DDoS attacks

DDoS as a category holds many disguises and continues to evolve, becoming challenging to detect and mitigate. What makes matters worse is that the internet is filled with poorly engineered networks, open resolvers and DNS proxies, creating platforms for attackers to penetrate and launch attacks. Better network viewpoints are required to efficiently detect and mitigate the elaborate world of cybercrime.

DNS is positioned at a unique network point, holding the key to valuable information to enable enhanced DDoS detection and prevention. As part of the automatic flow of network traffic, it observes all the application service requests for domain names and the associated 'hits', or requests for access to resource IP addresses and the responses to these requests in real time.

Aside from bringing down websites and networks, DDoS is frequently used to disguise deep cybercriminal activity such as fraud or theft of personal information; thus, rapid detection is utterly critical.

Turning up the volume

How is it possible that the conventional activity of translating domain names to IP addresses could have such a large blast radius? Besides the fact that User Diagram Protocol (UDP) is stateless and easily spoofed, it must respond when a user queries a server. This is a prime function of the resolution process. The simple query/response process is magnified by what's known as DNS amplification, a type of DNS-based DDoS attack.

A DNS amplification attack involves an attacker sending relatively small query packets to the resolver, which then replies with much larger responses, overwhelming the target victim. DNS query response sizes (~4,000 bytes) are much larger than the request size (~40 bytes). The attack is intensified due to the many open resolvers available to accept queries from any source and send responses to anyone. There is no license on the internet, which leaves a long list of unmanaged open resolvers, expanding the attack surface. These queries stress network resolvers which must go out and get answers.

Attackers realize that open DNS proxies on home gateways can be used as an additional tool in their arsenal to launch amplification attacks. In one DDoS attack in 2015, more than 300,000 home gateways were used over two days to generate nearly 300 million malicious queries per hour. An attacker sends packets with spoofed source addresses to an open DNS proxy on the home gateway, which the proxy queries to

the configured resolver. The resolver sees the queries coming from a known legitimate source and responds back to the home gateway, which forwards the spoofed source address to the unknowing target.

Due to high query volume, networks are adversely impacted and internet service for subscribers becomes degraded or goes offline.

How Nominum thwarts DDoS

Nominum Data Science continuously analyzes DNS data to expose malicious fingerprints and other trails from cybercriminals. One method the team employs is tracking domains generated by Domain Generation Algorithms (DGAs).

DNS-based attacks go through complicated movements and variations of patterns to avoid detection. A common theme attacks have is creating large spikes in queries and domain names, which often sound the alarm for Nominum Data Science to step in and investigate further. For example, a DDoS attack may include only a few domain names, but generate billions of queries that start and stop unpredictably, causing enormous spikes in traffic. The catch is these attacks will target both popular and obscure domains, making the attack difficult to verify right away. Typically, DDoS attacks are hidden among queries for relatively popular domains, which causes them to be overlooked as usual traffic. But if we dive deeper into the data, evidence of an attack becomes clear.

To thwart these attacks, the team analyzes the following patterns for potential further analysis:

- **New domain names.** Hundreds of thousands of new domain names might appear each day, particularly those with nonsensical names.
- **Domain name lengths.** Domains with 14 characters, 17 characters and 37 characters exceed what may be expected in a typical distribution. This type of character length may indicate some kind of malicious algorithm or machine-generated domain.
- **Frequency of queries against a domain.** Patterns may include an unusual spike in the frequency of queries and the number of clients querying domains.

Malware such as Mirai can commandeer IoT devices such as DVRs and use them as bots in massive malicious attacks such as the attack on October 21, 2016. As a side note, we anticipate larger DNS-based

//Tech notes

Nominum Data Science has developed unique algorithms to detect anomalies. One set of algorithms queries patterns to determine whether they match a specific profile of known malicious activity or not. Another set of algorithms then applies advanced machine learning techniques to these “anomalous” names to find the malicious activity.

These algorithms use attributes for each domain name to calculate a vector and measure how closely it compares with every other name. This process exposes subtle patterns that link different names to a single malware family. Names with similar vectors form what’s known as “clusters” that represent the output of a multi-dimensional feature matrix into a two-dimensional space. Each dot represents a domain, and the closer the dots are to each other the more similar they are. (See Chart 10 for visualization.)

CHART 9. **AMPLIFICATION QUERIES—FOUR OPEN RESOLVERS IN 1 NETWORK, 1 HOUR**

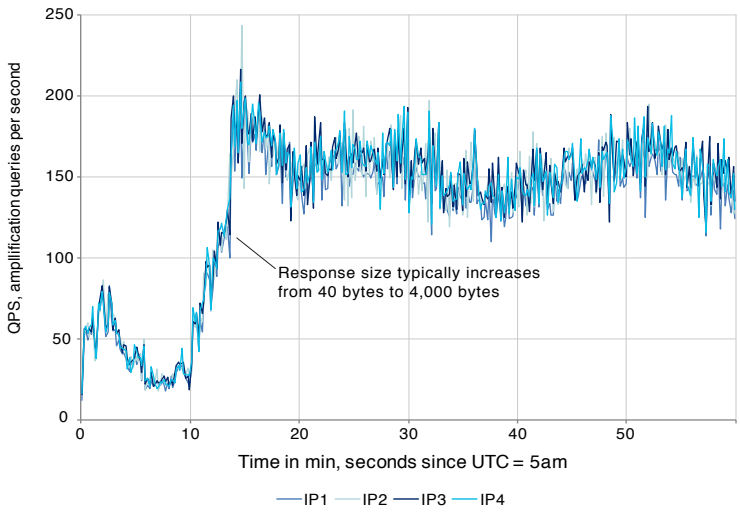
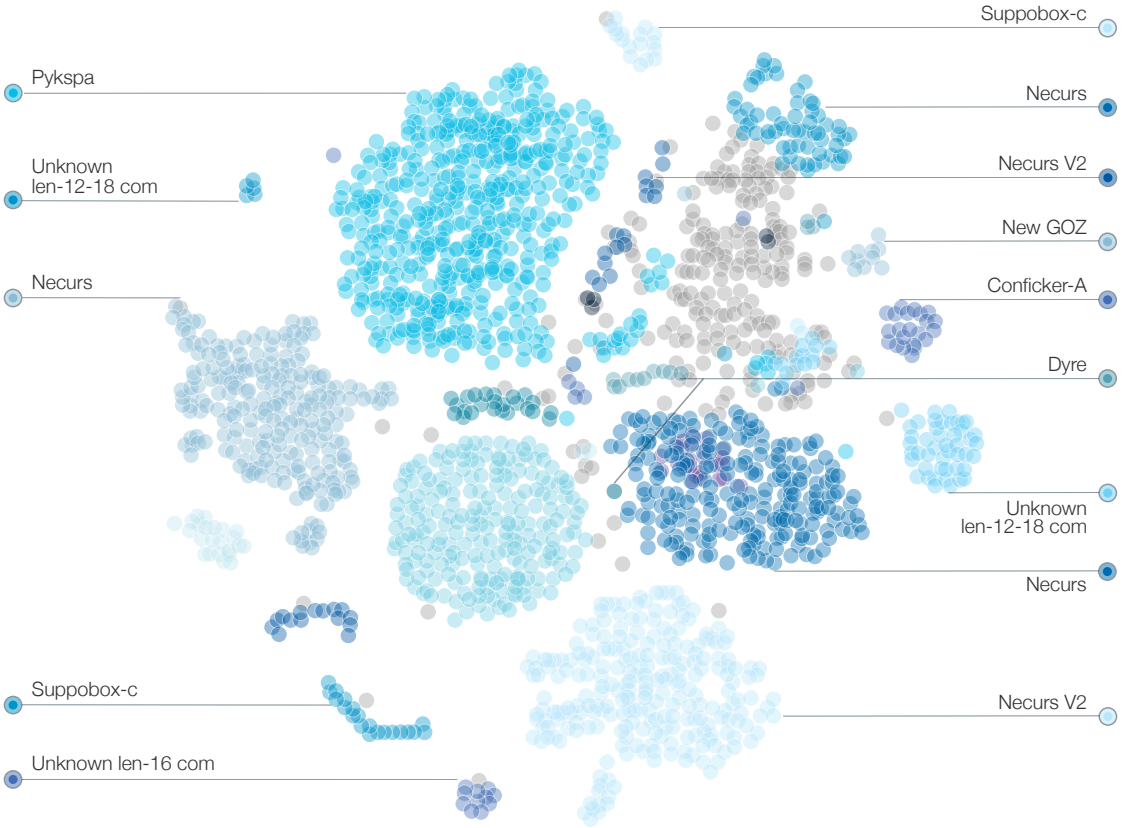


CHART 10. **CORRELATION TECHNOLOGY IDENTIFIES NAMES WITH COMMON CHARACTERISTICS**



DNS AMPLIFICATION ATTACK UNDER A TIME MICROSCOPE

While DNS amplification attacks are a popular type of reflection attack that use incorrectly configured network devices, network providers may not have easy-to-use tools to drill down and understand the evolution of an amplification attack with a per-second discretization.

We took one hour of a subnet from a network provider and found that four open resolvers were used in a single attack at 5:00 UTC on September 24, 2016.

The attack used the cpsc.gov website that belongs to the United States Consumer Product Safety Commission with a response size to ANY query of 4,454 bytes. This website is on our dual-purpose amplification domain that should not be blocked outright, as it is a legitimate website.

Two observations stand out. First, a single IP can produce up to 250 queries per second, and, if not protected against, can generate 4 GB per hour in an attack stream to a target. With millions of open resolvers around the globe, the strength of the DDoS attack can be quite high. Second, all four IPs exhibit a similar pattern with almost perfect correlation, indicating the same source of the queries. Without the rate-limiting policies available in Nominum N2™ ThreatAvert, this attack can generate large traffic exiting the network if the target is located outside (which is frequently the case), not to mention impacting the experience of affected subscribers.

threats to the domains that were attacked, as there appears to be a very high number of IoT devices under hacker control capable of executing DNS-based DDoS attacks. Nominum Data Science has added domains to N2 ThreatAvert that were used by the Mirai botnet to participate in these attacks.

Fits and starts: Pseudo Random Subdomain Attacks

Pseudo Random Subdomain (PRSD) attacks began to surface in 2014. They are an emerging style of DNS-based DDoS attack that threatens the DNS infrastructure. Similar to amplification attacks, the approximately 20 million open DNS proxies in consumer home gateways are utilized as an attack tool, but unlike amplification attacks, PRSD attacks directly target authoritative DNS servers without spoofing the source of the queries.

With PRSD attacks, the attacker generates queries using randomized labels prepended to target domains. The queries are first sent to open DNS proxies, which send to the configured resolver and then authoritative server. Every query is different, creating a constant flow of traffic between resolvers and authoritative servers. Because the names are random, they are never in cache, resulting in additional computational work and causing authoritative servers to crash.

This style of attack poses mitigation challenges as traffic between the resolver and authoritative server appears legitimate. As a result, many mitigation techniques employed to combat amplification attacks cannot be used to mitigate PRSD attacks.

To understand PRSD attacks, Nominum Data Science looked at data from April 2014 to September 2016, and noticed a spike in attacks in the November/

CHART 11. **PRSD ATTACKS UNEXPECTEDLY RISE AND FALL DURING THIS TWO-YEAR SAMPLE**

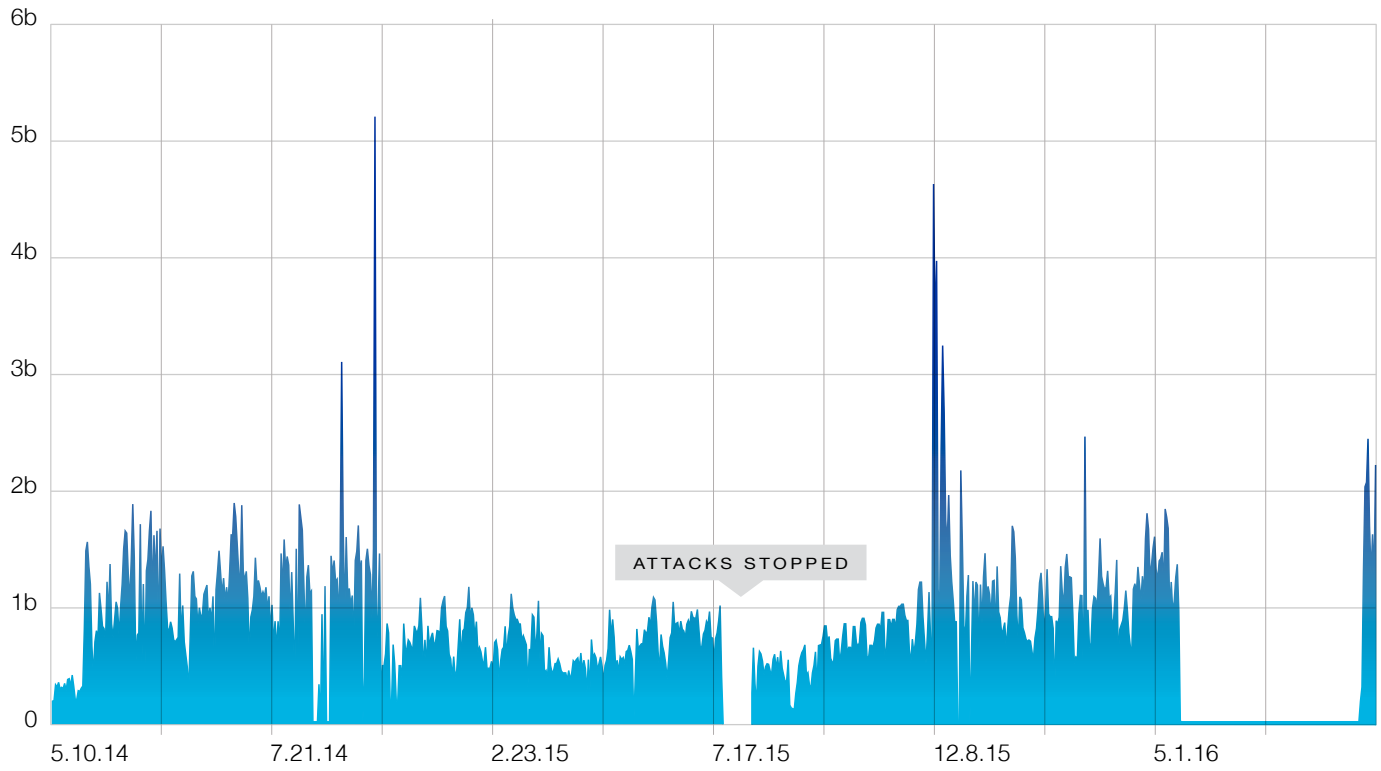
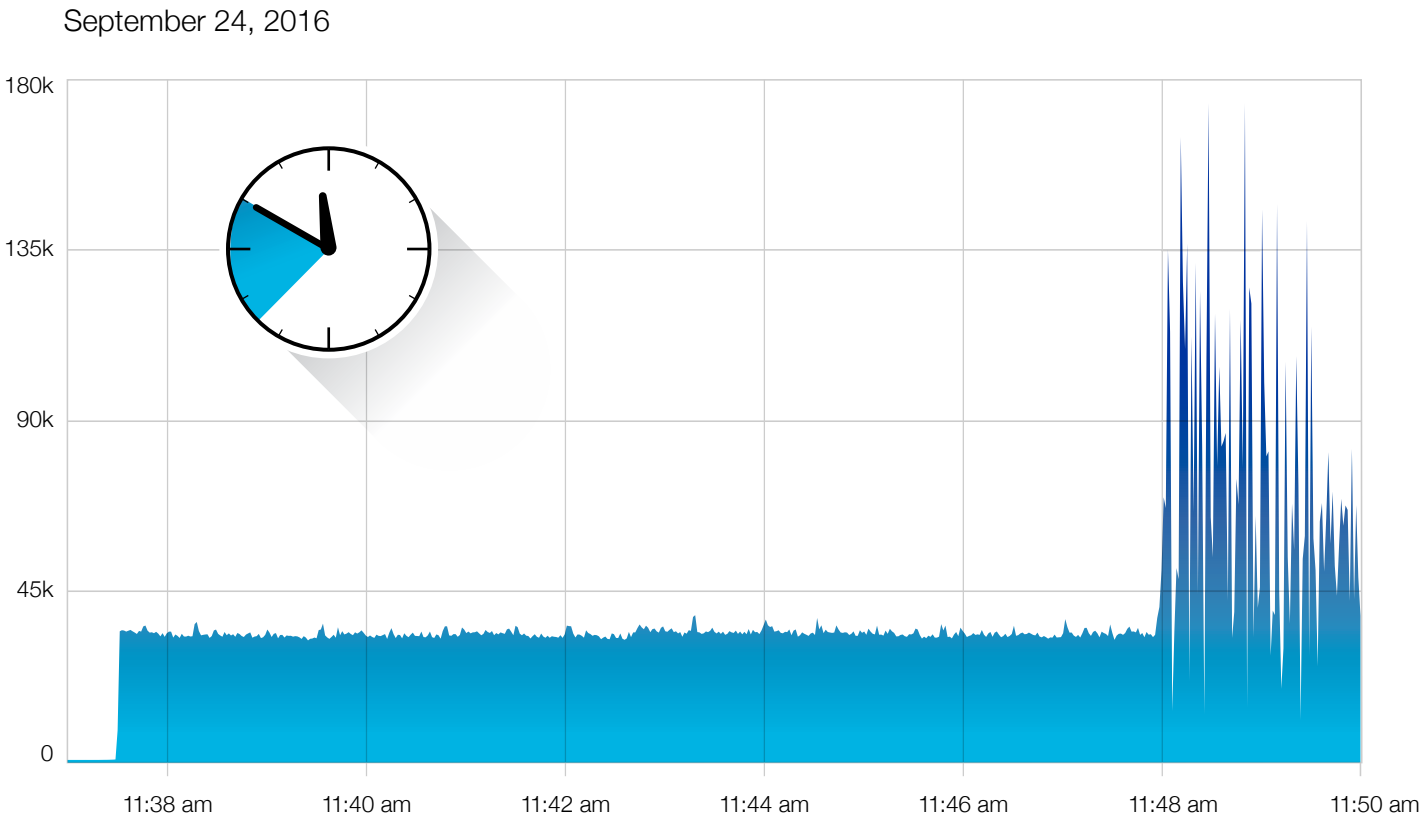


CHART 12. **A MINUTE-BY-MINUTE VIEW OF THE SEPTEMBER 24 PRSD ATTACK**



PRSD ATTACKS: FAST AND FURIOUS

PRSD attacks are known to be fast and furious. How fast? The graph above illustrates the first 10 minutes of a typical attack on a single network. The attack took place on September 24th, 2016, on a service provider network in South America, with the targeted victim being a Russian gambling site.

The Russian site saw exactly zero queries coming from the South American network from the day it was created until September 24th at 11h:36m:47s. The number of queries suddenly began to rise to approximately 40,000 queries per second in a matter of 10 seconds, and remained at this activity level for exactly eight minutes.

This was the initial stage of the attack, when the scripts generating the attack were "testing the waters." While 40,000 QPS (queries-per-second) are substantial, they are not enough to cripple a typical service provider network.

Then, at 11:48:10, the attack went into "full throttle" mode, blasting the network with a volume of 135,000-180,000 QPS. If not adequately protected, this is when a network will crash. Nominum Data Science, in its anomaly detection efforts, regularly analyzes QPS so suspected domains with high query rates are added into Nominum Global Intelligence Xchange (GIX) feed lists and automatically blocked from the network.

December 2015 timeframe. As outlined in this video from December 2015, attacks can generate more than 1.5 trillion queries to attack targets. More recent attacks have grown in sophistication, with many targeting larger, well-known brands rather than unknown domains.

PRSD personas

Our research of the malicious actors behind the PRSD attacks led us to believe that different attacks are generated by different attackers.

Type A

This group of cybercriminals primarily attack Chinese domain names, specifically targeting porn, gaming, gambling, and peer-to-peer sites; we believe the main motivation is extortion of payments to cease the attacks.

Type B

Another set of domain names under attack are peer-to-peer gaming sites popular in Europe and North America; we speculate the motivation is to block competing players from gaining an advantage.

Type C

We have seen evidence of domain names attacked by DDoS-for-hire services, probably for a wide range of motivations. This category includes U.S. schools and colleges, and some political sites.

Others

Finally, we have recently seen prominent U.S. and European companies under attack, including sites associated with financial services, pharmaceutical, web services, and other well-known international companies. With a wide range of victims, PRSD is a multinational, cross-industry type of attack.

Regardless of the end target, service providers around the world are innocent and unknowing victims as the attack traffic dramatically increases the load on their DNS infrastructure, and potentially brings it to a halt.

Combating Pseudo Random Subdomain Attacks

Nominum's mitigation technique involves blocking attack traffic using ingress filtering in resolvers. This technique is useful for the following reasons:

- Protects resolvers since they will not generate recursive responses.
- Reduces load on authoritative servers since they don't receive bad traffic from resolvers.
- Eliminates adverse impact of Response Rate Limiting, because resolvers don't forward bad traffic to authoritative servers.
- Can use fine-grained policies to protect legitimate queries for popular names.

As attacks inevitably escalate and evolve, dropping attack traffic at resolver ingress will become even more important for maintaining the operational integrity of the internet.

Nominum's N2 ThreatAvert product uses precision policies that contain familiar DNS-centric syntax to manage DNS traffic: fine-grained filtering, rate-limiting, truncated responses and more are at work to thwart PRSD attacks.

Holding subscribers hostage | the tidal wave of ransomware

In 2016, ransomware took center stage. While the first known ransomware was "PC Cyborg," written in 1989,[5] the rising use of bitcoin and advancement of encryption techniques have helped it escalate, today averaging 4,000 attacks.[6] While Locky consumed much of the media's attention, a plethora of other ransomware threats arose. This denial-of-access style attack prevents subscribers from retrieving files and is commonly used in conjunction with some kind of Trojan, penetrating the system through a downloaded file. A payload is run that encrypts the files until a ransom is paid through hard cash or bitcoins.

[5] http://www.welivesecurity.com/2015/09/18/evolution-ransomware-pc-cyborg-service-sale/

[6] http://www.wsj.com/articles/in-the-bitcoin-era-ransomware-attacks-surge-1471616632

The path to ransomware

The end goal of cybercrime has always been to turn cyber-assets into money. One way to get this done it to compromise a wide network of devices (using malware), and then offering paid services utilizing them (DDoS, spamming, malicious hosting, etc.). Another more direct way is through a banking Trojan, which collects online banking credentials on infected devices and uses them to transfer money from the victim's account. The process of moving money requires additional steps and usually involves additional parties such as 'money mules' which conceal the identity of fraudsters and act as intermediaries, transporting money between fraudulent parties.

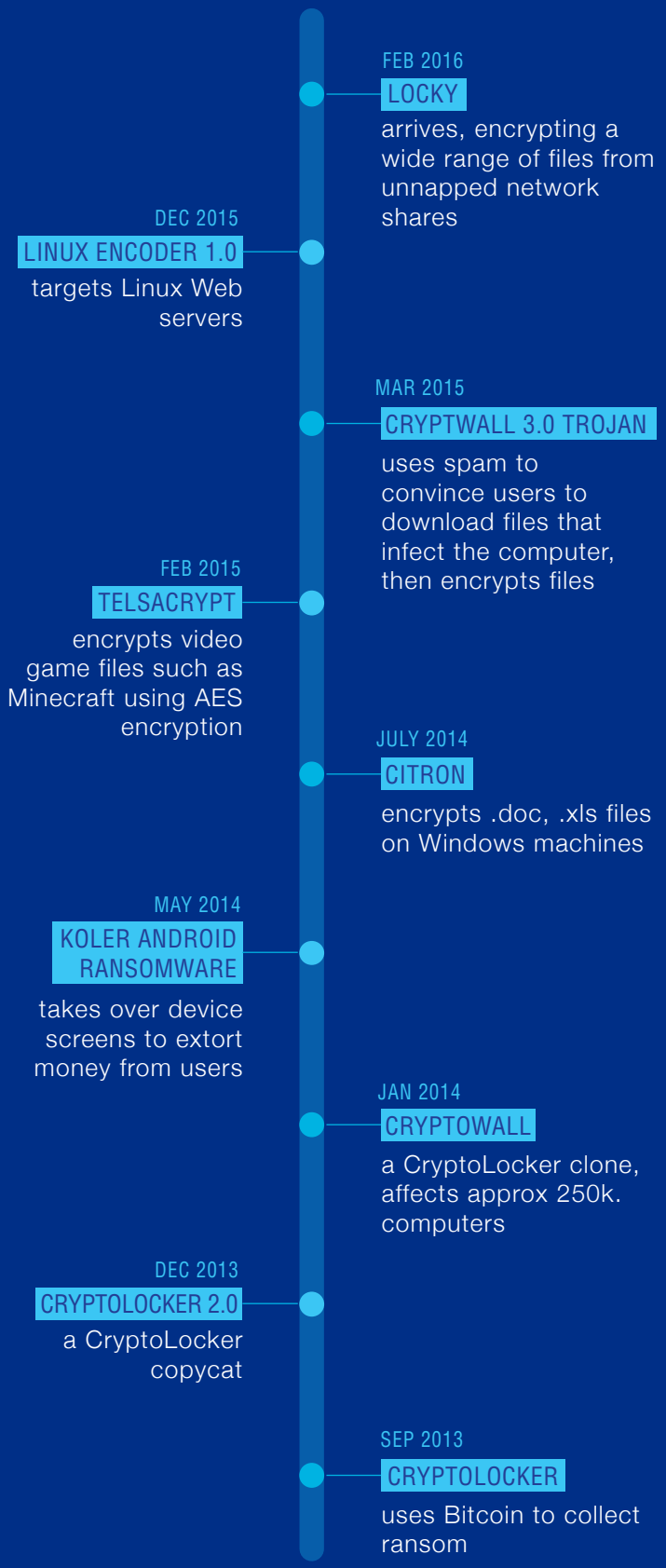
Ransomware emerged this year as the fastest and most efficient way to turn virtual assets into real money because it combines the best of the two worlds mentioned above: it infects a device to gain access to personal files and encrypt the data, and then 'translates' the infection into money through a ransom demand. This form of attack is considered an ideal form of cybercrime since it doesn't require additional partners and intermediaries. Additionally, because individuals and organizations are willing to pay the price for their data, this encourages cybercriminals to increase their efforts to launch more ransomware attacks and enhance ransomware tools. The ransom fee is set to a medium level—typically around $300 to $600—that most victims will pay to avoid the hassle of lost data.

Unlocking Locky

Locky is a notorious crypto ransomware enhanced by the ToR network and Necurs botnet infrastructure. It operates with the methodology "I've got the lock but do you have the key?" and has had a lot of success with a surprisingly high infection rate.

Locky encrypts data on infected machines, including mapped and unmapped network shares, and uses AES encryption, an advanced symmetric encryption algorithm. Disguised as a familiar JavaScript file, it comes as a report in a Microsoft Office document to

RANSOMWARE HIGHLIGHTS



LOCKY BY THE NUMBERS

Locky is as ubiquitous across the internet as it is effective, infecting nearly 100,000 devices per day, of which three percent submit payments. Cybersecurity experts estimate that Locky possesses 17 percent of the entire market share for all ransomware infections.

7 in 10
Malicious email attachments delivered by Locky in Q2 2016[1]

160
File types that can be encrypted by Locky (e.g., .docx, .jpeg, .xlsx)[2]

90,000
Devices infected daily around the world[3]

$459
Average ransom demand (BTC 0.5 to 1.00)[3]

$17,000
Largest Locky payout to date[3]

$1.6M per day
Average daily payout by Locky at the current bitcoin exchange rate[3]

[1] https://blog.barkly.com/ransomware-statistics-2016

[2] https://blog.avast.com/a-closer-look-at-the-locky-ransomware

[3] http://www.smartdatacollective.com/david-balaban/412688/locky-ransomware-statistics-geos-targeted-amounts-paid-spread-volumes-and-much-

the victim's email. The JavaScript file is not the actual payload, but acts as the downloader leading to Locky.

Most of the Locky infection files are distributed through spam campaigns, which are generated by Necurs. The amount of malicious traffic emerging from Necurs is staggering. According to MalwareTech, during the Necurs peak, there were over six million Necurs bots. Locky operates in a "master-troop mode"—the master being the C&C servers and the troops being the client bots. Once downloaded, Locky clients try to connect to the C&C to get a key to use for the encryption. The infected host may reach its C&C in a number of ways: direct IP communication, a number of fixed domains or by time-based DGAs that create random looking domains that are valid only for a few days.

Payments to cybercriminals are carried with a ToR browser. The ToR network conceals a user's identity by implementing a system known as Onion routing and relay technologies concealing user location and usage. Known as the dark web, it acts as a pre-built playground for malicious activity, making it impossible to trace back to the original source.

Disrupting the ransomware chain

Nominum Data Science automatically blocks known or emergent threats including Locky C&C communications, thus preventing the commander from communicating with its zombie army of infected devices. By identifying these botnet C&Cs, Nominum helps organizations to inform infected device owners and rapidly remove them from the "army."

//Tech notes

Using multiple clustering algorithms to analyze this vast data, combined with publicly available DGA algorithms, we are able to predict all the Necurs domains generated through DGAs, for all of Necurs' different variants. Nominum N2 ThreatAvert protects networks from Necurs by automatically blocking over 10,000 unique Necurs server domains.

The Locky DGA changes keys frequently, creating entirely new strings of domains. This means every key change extends the life of the exploit. Nominum Data Science came up with a method of blocking Locky C&C communications, so Locky bots cannot obtain encryption keys. Leveraging the reverse-engineered DGA and in-house developed algorithms, the seeds Locky uses to generate new domains can be discovered.

Chart 13 shows an example of domains that were generated by Locky malware authors. By adding to the threat list the domains that Locky will use in the future to obtain encryption keys, C&C communications can be blocked, and bots on client devices can't encrypt files. Every day or two Locky uses a new seed, changing the strings of domains it depends on to function. Names that a new seed will generate are proactively published to a threat list by N2 ThreatAvert; and since they are domains Locky will use in the future, this bot is prevented from obtaining encryption keys, and infected users' files can be protected.

CHART 13. **DOMAINS GENERATED BY LOCKY SEED 7773 ON JUNE 1, 2016**

srltqxebl.xyz	kkbhlnkrxkwohs.su	avaqarnsviotyr.click
juialjetmtaje.org	rqicebtuicolbv.org	vyugvhveiy.su
ifwbhlfh.click	gqiipleq.su	vywekkxgkfpju.info

4 COMPLEXITY RISING

"The complexity of things – the things within things – just seems to be endless. I mean nothing is easy, nothing is simple."

- ALICE MUNRO

THE EXPANDING SECURITY PERIMETER

Traditional enterprise security architectures have been fundamentally challenged by the rise of the mobile workforce, a dramatic increase in the number of connected IoT devices and the increasing sophistication and speed of attacks.

Mobile workforce

Today's workforce expects to be able to work anytime, anywhere from any device on any application. Bring Your Own Device (BYOD) involves users bringing personal devices onto a private network. This holds many network and security access control challenges as an increasing number of devices are joining and leaving the network. Often these devices will get infected while the user is outside the corporate network (e.g., while working from home), and then brings that infected device onto the corporate network. Securing the mobile workforce requires much more than stopping malware on end users' mobile devices. Even if mobile operating systems were 100 percent secure, the people who use them are not. Users receiving targeted phishing messages pretending to be from a customer or business partner can easily trick employees into disclosing sensitive user names and passwords that ultimately enable unauthorized access to company systems.

Internet of (insecure) Things

Mobility is unlocking productivity by connecting workers and devices to the internet. Traditionally, IP endpoints were restricted to certain types of devices. However, IoT completely changes this paradigm and gives everyday objects network connectivity. IoT objects now have unique identifiers with the ability to send and receive data without intervention. IoT has the potential to dramatically increase the productivity of industries as diverse at healthcare, transportation and agriculture and has become a mainstream part of enterprises. Since Nominum started tracking IoT activity in November 2014, we have seen more and more IoT connectivity. Point-of-sale terminals are internet-enabled to allow better tracking and inventory management. In transportation, trucks are now connected to the internet to allow for more sophisticated fleet, workforce and inventory management, for example.

Connecting an increasing number of systems to the internet unlocks productivity but at the same time dramatically increases the "attack surface" and creates new risks to the enterprise. In many cases, these devices aren't future-proofed, meaning endpoint security can't be installed on these devices, while network security products fail to properly detect malicious traffic from these devices.

The losing race

Compounding the rise of the mobile workforce and growing penetration of connected devices is the increasing sophistication and speed of malware. As this report describes above, millions of never-before-seen domain names are queried daily, the majority of which are suspicious. The end result isn't good.

Predictive intelligence and proactive protection

Nominum's N2 ThreatAvert solution is powered by predictive security intelligence. Today's sophisticated attacks routinely evade conventional after-the-fact technologies such as firewalls and signature-based detection. Therefore, it's essential to adopt new technologies such as N2 ThreatAvert that predictively neutralize these new threats. Nominum learns from internet activity patterns to identify attacker infrastructure being staged for the next threat.

A report by Lastline Labs indicates that 51 percent of zero-day malware is undetected by anti-virus solutions.

It is possible for Nominum Data Science to predict and prevent attacks before they're fully launched. It is also possible to stop C&C communications before they do real harm. This proactive protection requires:

- **An extremely large data set.** In the past 12 months, Nominum has analyzed over 20 petabytes of data from across the globe in order to determine the areas from which theats originate and uncover patterns of cybercriminals.
- **Proprietary data analytics and visualization tools that allow Nominum to effectively anticipate and block cyberthreats.** We combine human intelligence with machine learning to learn new patterns. Then, statistical models are applied to categorize these patterns, detect anomalies, and automatically identify known and emergent threats. We apply statistical models to real-time and historical data to predict domains that are likely malicious and could be used in future attacks. Specifically, we had more than three million domains in our threat intelligence feed with 200,000 domains added and deleted from the list daily on average from July to September 2016. Not only can DNS see the traffic very quickly; the time to protection can be dramatically reduced when advanced machine learning techniques are applied.

Where traditional security falls short

Many threats go undetected by traditional detection methods such as antivirus, DPI and sandboxing. A report by Lastline Labs indicates that 51 percent of zero-day malware is undetected by anti-virus solutions.

Threats such as DNS Amplification, Capshaw Trojan, Shylock Spybot, Necurs and PRSD attacks are not detected by traditional solutions. Because Nominum blocks communications with C&Cs, a highly effective security layer is added.

As the clock ticks

Timeliness is a critical factor in successfully mitigating attacks. Industry statistics on enterprise responsiveness to security breaches is concerning. For example, Verizon reports that 93 percent of data breaches took "seconds or minutes" to compromise a device with over 98 percent of data exfiltration happening within "days" of the compromise.[7]

By contrast, less than 20 percent of compromised organizations discovered the breach within "days."

[7] http://www.infosecurity-magazine.com/news/verizon-93-of-compromises-take/

THE CONNECTED HOME

NOW

6.4 billion
connected things [1]

34% of Americans own in-home IOT devices [2]

328 million things connect to the internet each month [3]

IN 5 YEARS

44 ZB of data
will be exchanged between connected devices by 2020 [4]

500 connected gadgets in a single home [5]

28.1 billion devices connected to the internet by 2020 [6]

CONSUMERS SAY

90% say security is one of the top reasons to purchase a smart home system [7]

71% fear that their personal information may get stolen [8]

57% fear that their smart home technology will have too many bugs [9]

[1] http://www.forbes.com/sites/gilpress/2016/01/27/internet-of-things-iot-predictions-from-forrester-machina-research-wef-gartner-idc/5/#5f0a1fe76a04
[2] http://www.theharrispoll.com/business/Consumers-Embrace-Smart-Home-Technology.html
[3] http://www.politico.com/agenda/story/2015/06/internet-of-things-growth-challenges-000098
[4] http://www.zdnet.com/article/the-internet-of-things-and-big-data-unlocking-the-power/
[5] http://www.zdnet.com/articleyoure-going-to-need-a-bigger-house-500-connected-gadgets-in-the-home-of-2022/
[6] http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated
[7, 8, 9] https://www.icontrol.com/wp-content/uploads/2015/06/Smart_Home_Report_2015.pdf

In other words, the horse leaves the barn before the rancher is even aware. Note: We don't intend to be fear mongers; we're saying threats are evolving, and that's usually because security companies are doing something right. That's why security is a game of cat and mouse. Once the effectiveness of a specific malware goes down, the bad guys need to evolve and solve new challenges.

The speed of threats today makes it clear that new approaches to defense are needed. These new approaches are found at the intersection of big data and machine learning.

A vast number of BYODs can connect to business networks, exposing them to risks not seen before.

Securing Guest Wi-Fi

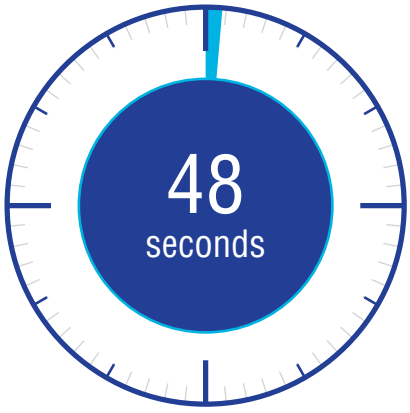
Guest or public Wi-Fi is a must-have for many businesses today, yet it comes with responsibility and risks. A vast number of BYODs can connect to business networks, exposing them to risks not seen before. DNS solutions like those from Nominum limit access in accordance with business guidelines and continuously protect against threats. Protection from phishing, viruses, spyware, adware and malware comes in the form of fine-tuned filtering that blocks bad traffic while allowing good traffic, providing businesses with both brand protection and assurance that guests have the best web surfing experience possible. DNS is vital in this area for automatic device detection and the application of policies when needed.

In summary, the mobile workforce, IoT and the speed of attackers has fundamentally challenged enterprise security. As a network-based technology that sees all outbound traffic, DNS should be a critical layer of defense in every enterprise.

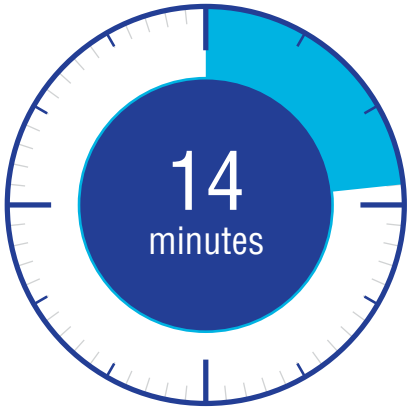
NOMINUM DATA SCIENCE: TIME TO DETECT THREATS

PREDICTED THREATS

DDoS ATTACKS



OTHER THREATS



EXPANDING ATTACK SURFACE

There are numerous factors at play in the expanding attack surface. In the same way that urban areas are experiencing overworked infrastructures due to poor city planning, so too are businesses facing unforeseen technological changes that provide distinct advantages yet introduce added security risk.

Cloud

In the early days of computing, applications were hosted on single machines, with patches and updates occurring on an individual basis (meaning there was much more control and isolation in the event of an infection). With cloud computing, applications are often split between on and off premise cloud locations, and as-a-service solutions continue to add complexity to the security perimeter. From Platform-as-a-Service to Infrastructure-as-a-Service, new hosting options are often cost-effective and provide much needed scalability yet they also give rise to new potential holes in the network. As we saw in Chapter 2, large cloud hosting services can unknowingly host malicious domains.

Overgrown networks

Enterprise networking started with simple designs consisting of standard sites, perimeter firewalling and static point-to-point connections to remote branch offices. The majority of connections were established internally and the network perimeter was more or less set in stone. Over time, components and users started to move, new technologies and devices were introduced and networking became more advanced. Complexity has been further amplified with the new cloud infrastructures, advanced high availability, multiple interconnects and more sophisticated traffic engineering requirements. As a result, the enterprise security perimeter has completely dissolved. It's now a given that there WILL be infected devices on the network—but detecting and remediating them is extremely challenging.

The original security model was created with a box-by-box framework, with centrally located firewalls, web gateways, IPS, IDS and AV software on hosts. In this structure, the deployment of security appliances and agents are within the perimeter, so malware must first enter the network for detection. Additionally, web gateways rely on HTTP traffic to perform, and with the variety of breach variations, they can't detect all attacks. What is needed—but is missing from enterprise networks—is a front defense layer to provide security enforcement directly at the edge of the network, no matter where the perimeter is. Effective security mechanisms must be in place to instantly detect infected devices and send immediate notifications to those infected.

Virtualization security paradigm change

Traditionally, the majority of traffic left the data center, known as North - South. With the advent of virtualization, the majority of traffic now stays inside the data center, East - West. The East - West profile changes the firewalling location. Stateful filtering tracking the state of the packet is now carried out closer to the workload. Before, this was performed in central locations with physical security devices—but the change from a centrally located security paradigm to a distributed model opens up new avenues for attack. Do these mini firewalls perform true stateful services and deep packet inspection or do they provide only partial protection? Stateful filtering enables better protection to partial or stateless as it tracks the specific TCP flags.

Micro-what?

In today's app era, a monolithic style single server/single application model has given way to a microservices architecture—with applications now being vulnerable to many different services potentially spread across multiple enterprise locations and cloud infrastructures. Microservices have a direct impact on the security architecture—with new end points, new ports, new API exposure, and more.

This puts pressure on the network and security infrastructure as all of these individual services require secure cross-communication and resolution. The traditional monolithic application set-up may have wasted resources, but it was static and easier to secure many smaller services spread over multiple locations. This new paradigm puts incredible pressure on security teams to identify and remediate threats before they become a problem.

5 A LOOK FORWARD

"I'm always interested in looking forward toward the future. Carving out new ways of looking at things."

-HERBIE HANCOCK

PROJECTIONS – THE NEXT 24 MONTHS

DNS is not only a mission-critical infrastructure used by all organizations; it also plays a crucial role in today's layered security design, particularly as the attack surface continues to expand. Since 90 percent of cyberthreats use DNS to launch malicious attacks, DNS offers a unique vantage point from which cyberthreats—and the patterns and techniques of cybercriminals—can be uncovered, as discussed in this report.

While this is a first step in curbing cybercriminal activity, there is science involved in understanding new patterns and threats to keep cybercrime at bay. In order to change the cybersecurity game, a proactive approach is the only way to stop malicious activity which means we need to be able to predict the future of cybercrime.

Ransomware continues to grow

The rise of ransomware can be attributed to several elements. The end goal of cybercrime has always been to generate money, and only the preferred techniques have changed over the years.

In order to generate money in 2015-16 you needed a simple way to get malware onto a victim's device, and a secure, anonymized payment system to move the ransom money from the victim to the attacker. All of these preconditions existed prior to 2015; malware, which encrypts files to be used for extortion, has existed for at least 10 years; phishing, as a method of malware distribution, is not a new invention; and the bitcoin system has been transferring virtual currency since 2009. So what's new?

There are several factors contributing to this "perfect storm" of malware, which we believe will continue to make this cyber-scam extremely popular over the next 24 months.

First, compared to all other cybercrime techniques, ransomware has emerged as the easiest and fastest way to transform a hack into monetary gain. The comparison is the key term here, since attackers are

constantly looking for the weakest link, the path of least resistance. While there used to be easier ways to obtain cyber-wealth, they have been blocked by either new security measures or new regulations, or they just became less efficient. With dwindling competition, ransomware has positioned itself as the best alternative, and is likely to remain so until new security techniques or technologies make it far less effective.

Also, the value and the perceived value of data stored on hard drives is now at an all-time high. As a result, people are more vulnerable to extortion and are more likely to pay ransom for unlocking their data. If a hacker encrypted someone's computer in 2002 and requested a sum of $500 in order to restore the data, the urgency to pay the ransom would have been far less significant. Back then, the victim would have had hard copies of important documents and photos, and in general, the population didn't have the same digital lifestyle that we have today. But today we put our whole lives on our computers, making the ransomware market a tremendous "business opportunity" for criminals.

Finally, cybercrime is a copycat business. Once attackers see a scam that is successful, they immediately imitate it. That is how ransomware went viral. It is also easier to get their hands on a good piece of ransomware source-code, which makes the barrier to entry low. Our prediction is that as long as there is no reasonable technological solution to ransomware, more copycats are going to enter the market and the ransomware phenomenon will only continue to grow.

DDoS attacks to become bigger and faster

We predict that the size and frequency of DDoS attacks, and specifically DNS-based DDoS attacks, are going to increase in the coming year. There are many factors pointing to this continuing trend.

The most obvious is that DNS-based DDoS attacks are in high demand and are easy to implement. It's a perfect supply and demand scenario. Cybercrime organizations or any competing entities have strong motivation to disrupt their opponent's operations or extort them, and DDoS is a great way to achieve this goal— the demand side. In order to launch an effective DNS-based DDoS, all that is needed is a list of open DNS resolvers, and a strong botnet to take advantage of this vulnerability— the supply side. With ample quantities of both supply and demand, the threat is likely to keep growing.

Another key contributor is the knowledge and skill sharing among the cybercrime community. This is not a new phenomenon, however, the bar gets lower every year with the ready availability of free tools and inexpensive online services that allow anyone with an internet connection to launch an attack. DDoS as a Service (DoSaaS) is another cheap way to overcome technical incompetence and launch an attack. The source code for Mirai, the malware that powered the IoT botnet responsible for the historically large DDoS attack against KrebsOnSecurity in September of this year has been publicly shared; it is very likely to be used in the near future by a horde of copycats.

> ..the availability of free tools and online services allows anyone with an internet connection to launch an attack.

This easy sharing of knowledge, skills and tools has already led to an increase in both the frequency and size of DDoS attacks this year alone, and there is no reason to believe that this trend will stop.

Botnet of Things

As discussed in Chapter 4, the most recent concern with IoT among security circles was that hackers could break into smart devices in order to inflict harm on their users. For instance, it would be fairly easy to hack a connected pacemaker and disable it, or hack a Tesla to make it inoperable or hack a connected home thermostat to take control of the inside temperature.

While these scenarios are still possible, the main security risk of IoT is quite different.

As became evident from the record-breaking DDoS attacks on KrebsOnSecurity (launched September 20, 2016) and on Dyn (October 21, 2016) which brought down Twitter, Netflix and other web properties, compromised IoT devices are turning out botnets that are many times larger and faster. This is by far the biggest security problem IoT presents.

IoT 'things,' once compromised, are ideal candidates for serving as pawns in a botnet army. First, they are inexpensive and there are countless numbers of them. Think cheap routers, IP cameras, digital video recorders… the list goes on and on. Second, these devices have poor security features and are easily hacked: most of them use a default password, which users do not tend to change, they are rarely patched for known security vulnerabilities, they rarely have any firmware updates, they have no anti-virus type software, which could detect and possibly block a malware infection—and perhaps above all else, human users don't really have a way to monitor the behavior of their 'things': there is no screen, there is no noticeable "suspicious behavior" that they could report; and there is little awareness of whatever happens with the 'things'.

It is safe to predict that until these points of weakness are addressed, we're going to see the emergence of the "botnet of things." These botnets are likely to be much larger than the computer-only botnets of today, and their power could be much more devastating. Only a year ago a 'heavy-weight' DDoS attack might have reached the size of 100 GBPS, yet today we are already seeing IoT-based DDoS attacks of 650 GBPS. It is not unreasonable to believe that we'll see a 1 TBPS attack in the coming year. According to Gartner, 6.4 billion connected "things" will be in use by the end of 2016, a 30 percent increase from 2015.

It is worth noting that until IoT security can be handled through the endpoint, network-based security is the best way to block IoT threats. By observing network traffic (which includes DNS queries) generated by IoT devices, it is possible to identify malicious behaviors and block them at the network level.

N2 ThreatAvert

As botnets and other malware become more adept at avoiding detection and remediation, new strategies need to be used to combat them. Many of the new malware strategies make traditional malware block lists less effective. By using DGAs with changeable seeds, security researchers must constantly find new seeds to pre-generate domains, and by changing domain names rapidly, the information on lists very quickly becomes stale.

Nominum uses the DNS query data provided by our customers to detect and track the evolution of generated domains through a variety of algorithmic methods such as clustering, reputation scoring, and additional methods that continue to evolve. Recent innovations include anomaly detection algorithms, new domain clustering and a Domain Reputation System that blocks almost 100,000 domains daily. By employing these advanced methods, suspicious domains are detected very quickly and with high accuracy. False positives are weeded out automatically. N2 ThreatAvert now automatically blocks domains such as C&Cs and domains used by the Mirai botnet suspected of participating in the October 21 Dyn DDoS attack.

As threats and malware authors continue to innovate, so too will Nominum Data Science. Our global team of experts shares a relentless determination to protect unsuspecting victims from cyberthreats while providing the most secure DNS in the world, with no compromise in output or performance.

nominum™

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