Report

McAfee Labs
Threats Report

December 2016

intel Security

About McAfee Labs

McAfee Labs is one of the world’s leading sources for threat research, threat intelligence, and cybersecurity thought leadership. With data from millions of sensors across key threats vectors—file, web, message, and network—McAfee Labs delivers real-time threat intelligence, critical analysis, and expert thinking to improve protection and reduce risks.

McAfee is now part of Intel Security.

www.mcafee.com/us/mcafee-labs.aspx

Follow McAfee Labs

Introduction

It has been a rather eventful fall at Intel Security!

In late August, Intel security researchers joined with global law enforcement agencies to take down the WildFire ransomware botnet. In addition to assisting with the takedown, Intel Security developed a free tool that decrypts files encrypted by WildFire. Learn more about the WildFire ransomware and how to recover from it.

On September 7, it was announced that Intel Security will be partially spun off from Intel next spring, creating one of the largest independent pure-play cybersecurity companies in the industry. Although Intel will still own 49% of Intel Security, the majority will be owned by TPG, a leading alternative asset company. We will once again be known as McAfee.

Chris Young, Intel Security’s Senior Vice President and General Manager since 2014, will become CEO of the new McAfee. Our corporate product strategy, announced at the FOCUS 15 Security Conference last year, will not change. We believe that this change will position McAfee for enhanced focus, innovation, and growth. Exciting times!

In October, we announced and published the report *Health Warning: Cyberattacks are targeting the health care industry*. In that report, we examined health care data theft, including what is being stolen, who is stealing it, and what they are doing with it. The theft of personal medical data is particularly alarming because it cannot simply be canceled and replaced like payment cards. And the theft of medical research data threatens the economic model of the entire pharmaceutical industry.

In early November, we held our FOCUS 16 Security Conference in Las Vegas. Attendees were treated to more than 90 breakout sessions, 12 targeted group meetings, and dozens of TurboTalks. Ted Koppel, anchor of "Nightline" for 25 years and author of the bestseller *Lights Out*, spoke during a keynote about the possibility of a cyberattack on America's power grid and how to protect against it. The lights stayed on for us, so we had fun with the Goo Goo Dolls on the last night.

We also published our *McAfee Labs 2017 Threats Predictions report* last month. In that report, we offered 14 threat predictions around such topics as ransomware, hardware threats, hacktivism, and threat intelligence sharing. We also interviewed dozens of thought leaders from across Intel Security to develop long-range predictions around cloud threats and IoT threats. What threats and breaches do we expect to see? How will geopolitical issues, legislation, and regulatory actions affect these environments? And what responses do we anticipate from cloud service providers, IoT device developers, and security vendors? Read our report to find out.

And now we enter the holiday season by publishing the *McAfee Labs Threats Report: December 2016.* In this quarterly threats report, we highlight three Key Topics:

- Intel Security commissioned a primary research study to gain a deeper understanding of the ways in which enterprises are using security operations centers, how they have changed over time, and what they will look like in the future.
- Our second Key Topic summarizes the year in ransomware. Not only was there a huge jump in the number of ransomware attacks in 2016 but we saw significant technical advancements, too. We detail some of those advancements in this story.
- Finally, our third Key Topic digs into Trojans that infect legitimate code and hide out, hoping to go unnoticed as long as possible to maximize payouts. We show how attackers are creating long-lasting, fully undetectable malware.

These three Key Topics are followed by our usual set of quarterly threat statistics.

And in other news...

Zero-day malware continues to grow geometrically. Traditional antivirus software relies primarily on signatures to detect malware, but signatures are not useful for battling zero-day malware. To address this challenge, McAfee Labs has developed new proactive technologies designed to detect zero-day attacks.

- McAfee Real Protect is a machine-learning technology that incorporates statistical correlation to proactively identify malware without using an antivirus signature. It was first released in 2015 as free "beta" software both in McAfee Stinger and as a standalone application. This month, it will be released as a supported feature within McAfee ENS 10.5. As part of our flagship enterprise endpoint product, it will be supported and can be installed and managed from the McAfee ePolicy Orchestrator platform.
- Dynamic Application Containment limits or eliminates suspicious applications from making changes on the endpoint. It can block file or registry actions, child process creation, and injection into other processes. It can simultaneously save the first system targeted by attackers, prevent network infection, and provide business continuity to the endpoint. It is now part of McAfee ENS.

Every quarter, we discover new things from the telemetry that flows into McAfee Global Threat Intelligence (McAfee GTI). The McAfee GTI cloud dashboard allows us to see and analyze real-world attack patterns that lead to better customer protection. This information provides insight into attack volumes that our customers experience. In Q3, our customers saw the following attack volumes:

- McAfee GTI received on average 44.1 billion queries per day in Q3.
- McAfee GTI protections against malicious URLs decreased to 57 million per day in Q3 from 100 million per day in Q2.
- McAfee GTI protections against malicious files increased to 150 million per day in Q3 from 104 million per day in Q2. A year ago we saw a decrease in this period.
- McAfee GTI protections against potentially unwanted programs showed a small increase from Q2 to Q3. However, there was a dramatic drop in Q3 2016 compared with Q3 2015. In Q3 2016, we saw 32 million per day versus 175 million per day in Q3 2015.
- McAfee GTI protections against risky IP addresses showed a slight decrease, to 27 million per day in Q3 from 29 million per day in Q2. This was a much smaller decrease than the one seen from Q2 to Q3 in 2015.

We continue to receive valuable feedback from our readers through our Threats Report user surveys. If you would like to share your views about this Threats Report, please click here to complete a quick, five-minute survey.

Happy holidays to you and your loved ones.

—Vincent Weafer, Vice President, McAfee Labs

Contents

McAfee Labs Threats Report
December 2016

This report was researched and written by:

Christiaan Beek
Douglas Frosst
Paula Greve
Barbara Kay
Bart Lenaerts-Bergmans
Charles McFarland
Eric Peterson
Raj Samani
Craig Schmugar
Rick Simon
Dan Sommer
Bing Sun

Executive Summary

Do you need to pull up your SOCs?

Intel Security surveyed security practitioners to better understand how enterprises are using SOCs, how they have changed over time, and what they will look like in the future. Among other things, we learned that most organizations are overwhelmed with alerts, but they are making steady progress toward SOCs that are proactive and able to systematically respond to confirmed attacks.

Intel Security commissioned a primary research study to gain a deeper understanding of the ways in which enterprises are using security operations centers (SOCs), how they have changed over time, and what they will look like in the future. We interviewed almost 400 security practitioners across several geographies, industries, and company sizes. We learned that:

- Almost nine out of 10 organizations report that they have an internal or external SOC.
- Most are progressing toward the goal of a proactive and optimized security operation, but 26% still operate in reactive mode, with ad-hoc approaches to security operations, threat hunting, and incident response.
- 64% of organizations surveyed receive some type of security operations assistance from managed security services providers.
- About two-thirds of the organizations surveyed use a security information and event management (SIEM) solution. About half of those without a SIEM intend to deploy the functionality within the next 12–18 months.
- Most organizations are overwhelmed by alerts, and 93% are unable to triage all relevant threats.
- More than 65% of organizations have formal threat-hunting operations.
- The highest priority for future growth is to improve the ability to respond to confirmed attacks, which includes coordination, remediation, eradication, and preventing reoccurrences.

A year at ransom

Not a day went by in 2016 in which ransomware did not make security industry headlines. In this Key Topic, we highlight 2016's many significant technical enhancements in ransomware and the progress the security industry is making to fight back against the threat.

In last year's *McAfee Labs 2016 Threats Predictions Report*, we claimed that 2015's spike in ransomware attacks would continue and that ransomware would be a major and rapidly growing threat in 2016. As predicted, 2016 may be remembered as "the year of ransomware," with both a huge jump in the number of ransomware attacks and significant technical advances in this type of attack. Through the end of Q3, the number of new ransomware samples this year totals 3,860,603, an increase of 80% since the beginning of the year. Some of 2016's most significant technical advancements in ransomware include partial or full disk encryption, encryption of websites used by legitimate applications, anti-sandboxing, more sophisticated exploit kits for ransomware delivery, and ransomware-as-a-service. This Key Topic discusses these advancements and also some good news, including the newly formed anti-ransomware collaboration No More Ransom! and several successful ransomware control system takedowns.

"Trojanized" legitimate software is on the rise

In this Key Topic, we detail some of the many ways in which attackers place Trojans within commonly accepted code and how they remain below the radar. We also recommend policies and procedures that will help protect against this form of attack.

"Backdoor" access to systems has been coveted by malware authors, spies, and nation-states for decades. Tactics for finding this entrance range from persuading victims via social engineering to hand over the keys to their devices, to intercepting hardware in the supply chain and inserting backdoors to surreptitiously gain remote access. However, the most common method is through the deployment of Trojan software. Trojans infect legitimate code and hide, hoping to go unnoticed as long as possible to maximize payouts. In this Key Topic, we detail some of the many ways in which attackers place Trojans within commonly accepted code and how they remain below the radar. We also recommend policies and procedures that will help protect against this form of attack.

Key Topics

Do you need to pull up your SOCs?

A year at ransom

“Trojanized” legitimate software is on the rise

Share feedback

Security Operations Center (SOC)

A SOC is a facility in which information systems (websites, applications, databases, data centers and servers, networks, desktops, and other endpoints) are monitored, assessed, and defended.

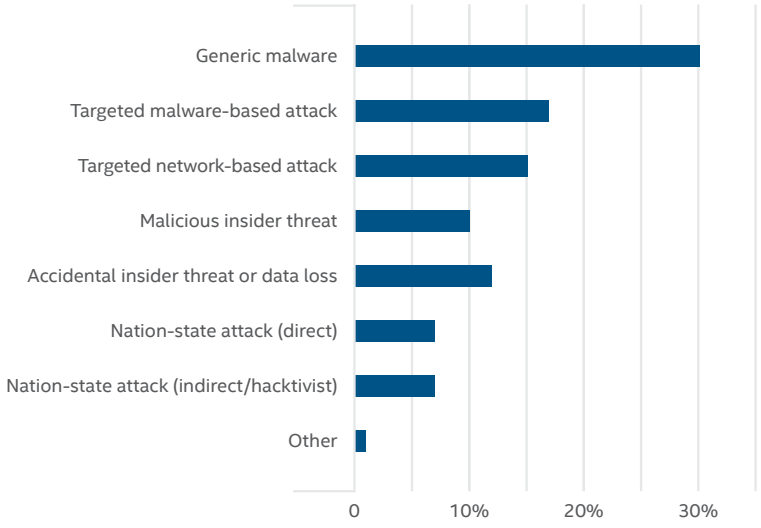
Do you need to pull up your SOCs?

The current state of and future plans for the security operations center

—Douglas Frosst, Barbara Kay, Bart Lenaerts-Bergmans, and Rick Simon

A few years ago, dedicated security operations centers (SOCs) seemed to be going the way of the dinosaur—the era of big rooms with big monitors and teams of analysts seemed ready to be replaced by distributed teams, outsourced, or disbanded entirely. If you were not in the defense department or on Wall Street, many thought, then you did not need a SOC. Then targeted attacks and insider threats moved from movie and government plots to an everyday reality for enterprises. According to an Intel Security survey, 68% of investigations in 2015 involved a specific entity, either as a targeted external attack or an insider threat.

Reason for security investigations



Source: Intel Security.

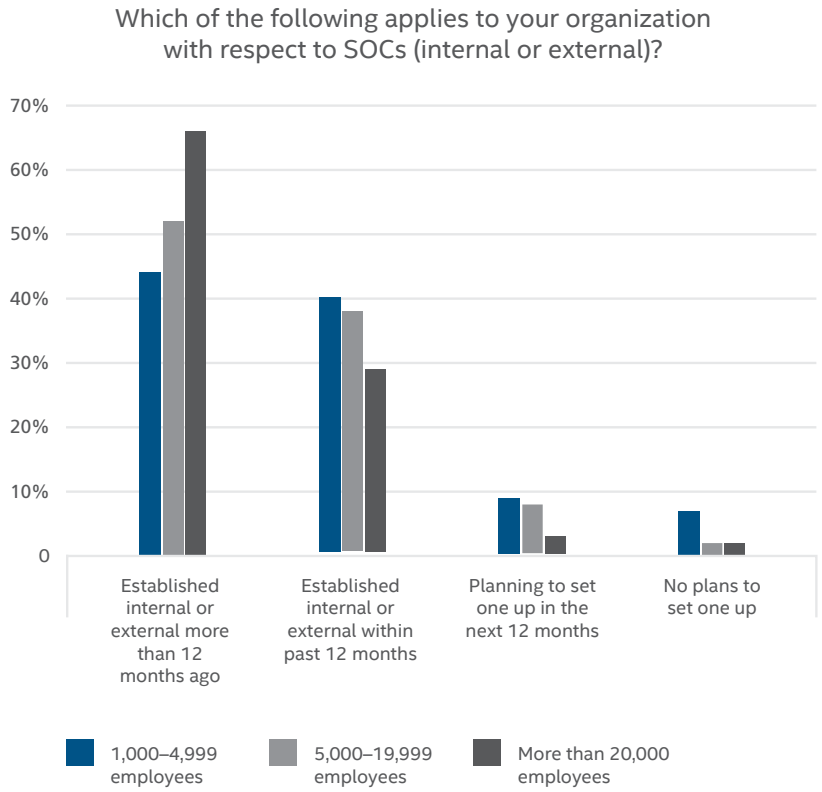
Almost all commercial and enterprise organizations run some type of SOC. They are investing more in SOCs and many have seen a decline in incident investigations. They attribute the decline to better protection and processes.

Today, almost all commercial (1,000–5,000 employees) and enterprise (more than 5,000 employees) organizations run some type of SOC, and half of them have had one for more than a year, according to the latest research study from Intel Security. As the number of incidents continues to increase, security organizations appear to be maturing and using what they learn to educate and improve prevention in a virtuous cycle. For instance, survey respondents documented their expanding investments in SOCs and attributed an increase in investigations to an improved ability to detect attacks. Those who reported a decline in investigations of incidents attributed this improvement to better protection and processes, which mature organizations perform as the final stage of a security investigation.

These are some of the findings in a primary research study commissioned by Intel Security on the current state of security management environments and threat detection capabilities, as well as priority areas for future growth.

Security management environment

Almost nine out of 10 organizations in this study reported that they have an internal or external SOC, although commercial organizations are slightly less likely to have one (84%) compared with enterprises (91%). Smaller organizations in general are implementing SOCs a bit later than enterprises, as only 44% of commercial groups have had one for more than 12 months, whereas 56% of enterprise SOCs have been around for that long. Most SOCs (60%) are currently run internally, with 23% operating a mix of internal and external support, and 17% fully external. For the few that have not established a SOC, only 2% of enterprises have no plans to do so, versus 7% of commercial companies.



Source: Intel Security.

Variety of SOC models

Companies run SOCs in a variety of styles. The study used the following definitions for five distinct operating models, listed here in increasing order of maturity:

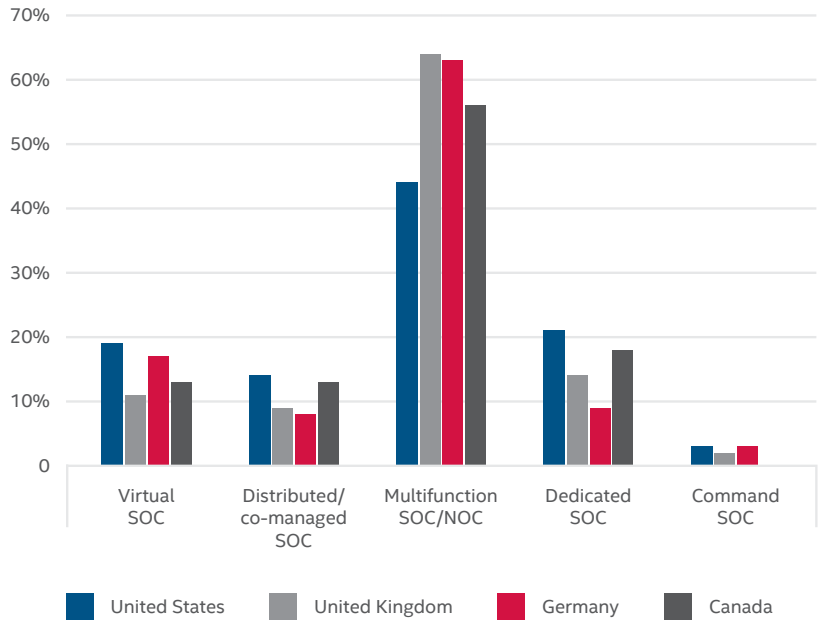
- **Virtual SOC**: No dedicated facility, part-time team members, reactive; activated only when a critical alert or incident occurs; primary model when fully delegated to a managed security services provider (MSSP).
- **Distributed/Co-managed SOC**: Dedicated and semidedicated team members; typically operates during standard business hours (8 hours per day/5 days per week); co-managed if used with an MSSP.
- **Multifunction SOC/NOC**: Dedicated facility with a dedicated team performing not just security, but other critical IT operations 24/7 from the same facility to reduce costs.

- **Dedicated SOC**: Fully in-house, 24/7 operations with dedicated facility and a dedicated team.
- **Command SOC**: Coordinates other SOCs, provides threat intelligence, situational awareness and additional expertise; typically not involved in day-to-day operations.

About half of organizations that have a SOC combine SOC and NOC functionality. 15% have dedicated SOCs and 15% have virtual SOCs.

Of the 88% of organizations operating a SOC, the majority (56%) reported that they use a multifunction model combining SOC and network operations center (NOC) functionality. Organizations in the United Kingdom (64%) and Germany (63%) are even more likely to operate in this model. Dedicated SOCs are in use by 15% of companies and are more prevalent in the United States (21%). Virtual SOCs are the third model, also used by about 15% of respondents, followed by a distributed or co-managed SOC, at 11%. Only 2% reported operating a command SOC.

Which one of the following five types of SOC models comes closest to describing your organization's SOC?



Source: Intel Security.

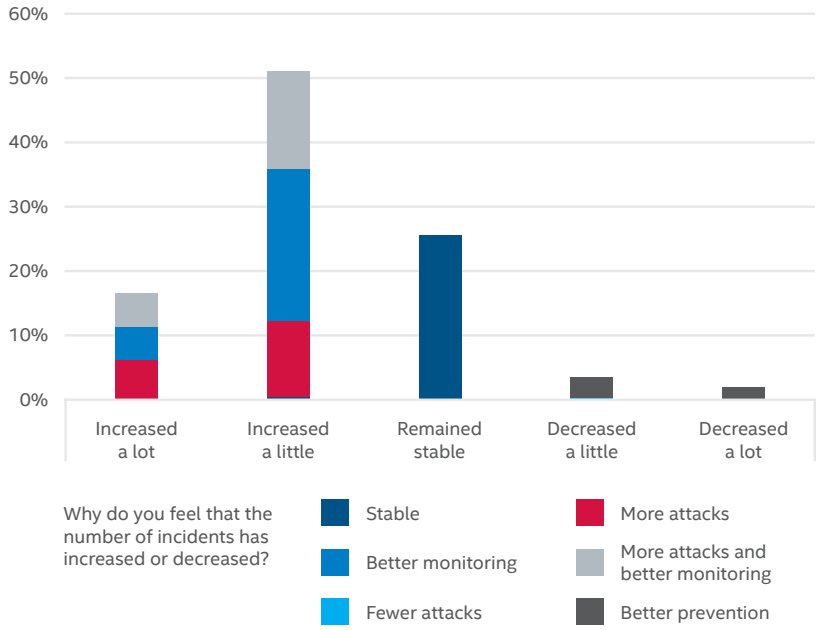
More than a quarter of surveyed businesses still operate in reactive mode, with ad-hoc approaches to security operations, threat hunting, and incident response.

This distribution of SOC implementations has several implications. The majority operate at or past the midpoint of SOC maturity, progressing toward the goal of a proactive and optimized security operation. However, more than a quarter (26%) still operate in reactive mode, with ad-hoc approaches to security operations, threat hunting, and incident response. This can significantly extend detection and response times, leaving the business at greater risk of significant damage, as well as facing a higher cleanup cost.

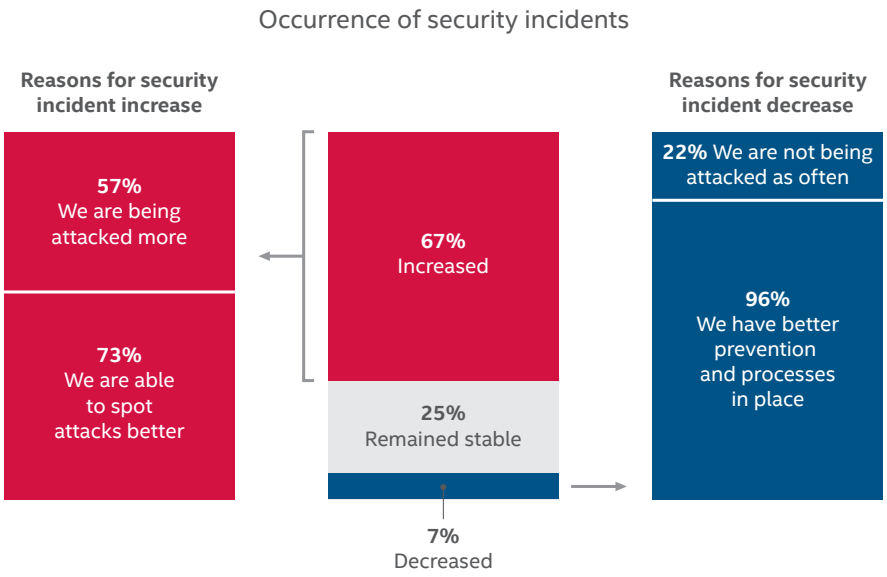
Increase in detected incidents

Whether from an increase in attacks or better monitoring capabilities, most companies (67%) reported an increase in security incidents, with 51% saying they have increased a little, and 16% that they have increased a lot. This is analogous to findings from the key topic "Information theft: the who, how, and prevention of data leakage" in the *McAfee Labs Threats Report: September 2016*. That primary research study found that organizations which watched data more closely for leakage reported more data-loss incidents.

Would you say that the number of security incidents your organization has encountered has increased or decreased over the last 12 months?



Source: Intel Security.



Source: Intel Security.

Only 7% overall indicate that incidents have decreased, and the remaining 25% say that they have remained stable over the past year. There was little variance reported by country, but incidents increased as organizations get smaller, possibly indicating that criminals have broadened their attack targets. Only 45% of the largest organizations (more than 20,000 employees) reported an increase, compared with 73% of the smallest (fewer than 5,000 employees).

The small group that reported a decrease in incidents overwhelmingly (96%) believe that this was due to better prevention and processes. Of those who said that incidents increased, the majority feel that it was due to a combination of improved detection capabilities (73%) and more attacks (57%).

Managed security services

About two-thirds of organizations surveyed receive some type of security operations assistance from managed security services providers. Choosing internal or external resources for security operations is most likely dependent on the availability of internal personnel, external services, and the comparative skill levels.

Most organizations receive some type of security operations assistance from managed security services providers, with 64% of those surveyed using MSSPs to augment their internal capabilities. Of the 26% that do not use external services, Canadian organizations are the least likely to use one, at 40%. The largest organizations are also more likely to go it alone, at 38%. For those that use MSSPs, the median work with two service providers. German organizations are more likely to use three, and Canadian organizations only one.

Reasons for an increase in MSSP use	Respondents choosing this as the primary reason
Improve investigations and scoping of potential incidents	14%
Security monitoring and monitoring coverage	21%
Improve advanced threat detection	18%
Help with SOC, incident response and hunter staffing, and skills shortages	18%
Access to technology such as big data platforms, analytics, and threat intelligence	12%
Dedicated incident response	8%
Compliance	4%
Reduce costs	3%
Device management	3%

Reasons for a decrease in MSSP use	Respondents choosing this as the primary reason
Improve incident response	20%
Improve the quality of investigations	13%
Improve the speed of investigations	15%
Reduce costs	20%
Improve security monitoring	23%
Improve compliance	3%
Access data and intelligence that is difficult to obtain from MSSPs	8%

For the next 12 to 18 months, most organizations (71%) expect their MSSP use to remain the same, while 19% expect it to increase and 10% expect it to decrease. Those that expect MSSP use to decrease are bringing more security operations in house to improve incident response and the quality of investigations. Those that expect it to increase are looking to external partners to improve investigations and scoping of potential incidents, and broaden security monitoring and monitoring coverage. Basically, choosing internal or external resources for security operations is most likely dependent on the availability of internal personnel, external services, and the comparative skill levels. As a result, there is some variance by country, with German organizations primarily interested in improving advanced threat detection with MSSPs, and UK outfits looking for help with technology such as big data platforms, analytics, and threat intelligence.

Security information and event management

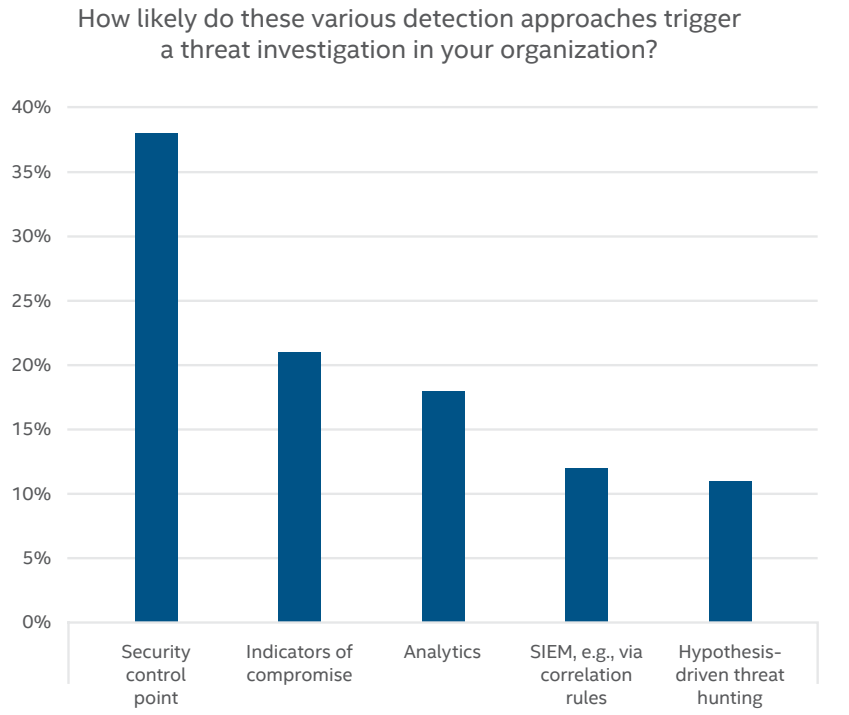
The ability to quickly identify, investigate, and resolve threats is probably the most important aspect of today's security operations. Preventing 100% of attacks may never be achievable, but security information and event management (SIEM) often provides a real-time understanding of the world outside—threat data, reputation feeds, and vulnerability status—as well as a view of the systems, users, data, risks, and activities inside, obtained through continuous monitoring and correlation. Actionable intelligence and situational awareness delivered by a SIEM may help orchestrate security operations and, when an incident is detected, may enable better collaboration for faster incident response.

Almost 70% of these organizations report using a SIEM solution today. Those organizations using external security services are highly likely (93%) to have those services involved with the SIEM in some fashion, most of them (71%) asking the MSSP to run day-to-day SIEM operations. Almost half (45%) of companies without a SIEM intend to deploy the functionality within the next 12 to 18 months.

Threat detection capabilities

The most common threat detection signals for about two-thirds of organizations surveyed come from traditional security control points, such as antimalware, firewall, and intrusion prevention systems. Just under half also rely on indicators of compromise or network analytics.

Increasing visibility and reducing detection and incident response times are key focus areas for most organizations, as they work to increase the maturity level of their security operations. Tried and true security methods continue to work, and are still the primary source of information. The most common threat detection signals for a majority of organizations (64%) come from traditional security control points, such as antimalware, firewall, and intrusion prevention systems. Just under half (46%) also rely on indicators of compromise to search for a breach, or using network analytics (40%). A few (26%) have begun using a SIEM to correlate events and identify potential incidents, and 23% are actively hunting attacks.

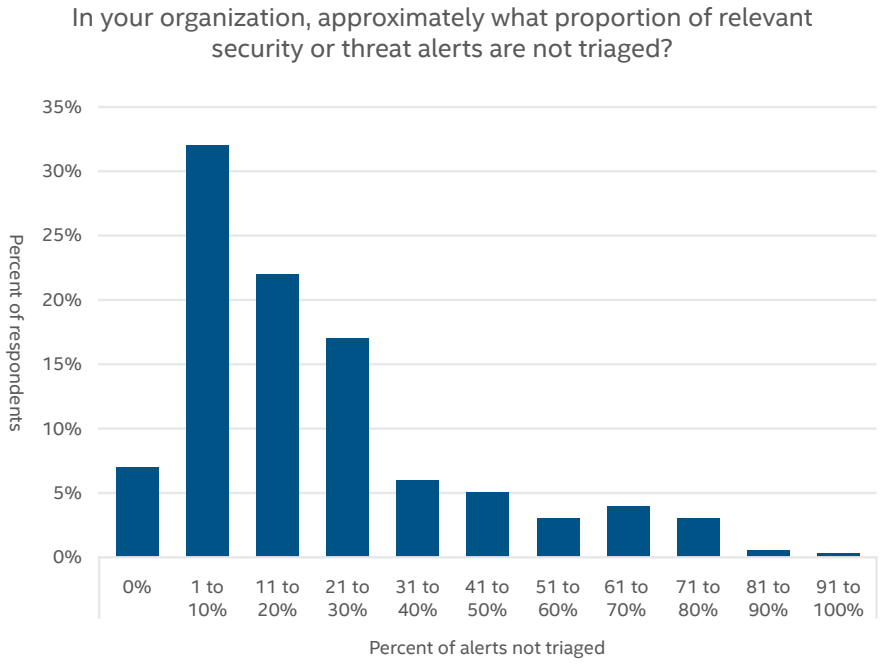


Source: Intel Security.

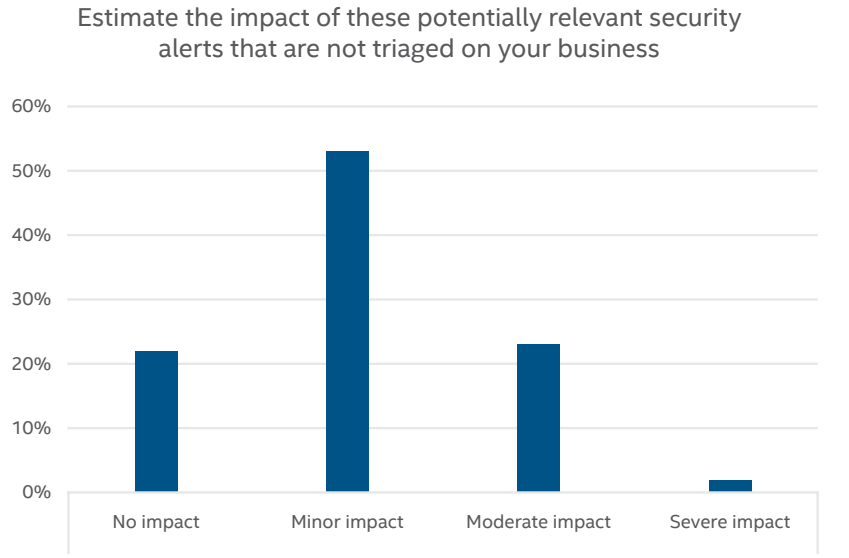
Alert volume and investigations

Most organizations are overwhelmed by alerts, and 93% are unable to triage all relevant threats. On average, organizations are unable to sufficiently investigate 25% of their alerts, with no significant variation by country or company size. Almost one quarter (22%) feel that they were lucky to escape with no business impact as a result of not investigating these alerts. The majority (53%) reported only minor impact, but 25% say they have suffered moderate or severe business impact as a result of uninvestigated alerts. The largest organizations, perhaps because of their better monitoring capabilities and stable incident levels, are more likely to report no business impact (33%).

Most organizations are overwhelmed by alerts, and 93% are unable to triage all relevant threats. On average, organizations are unable to sufficiently investigate 25% of their alerts. Almost one-quarter feel that they were lucky to escape with no business impact as a result of not investigating these alerts.



Source: Intel Security.

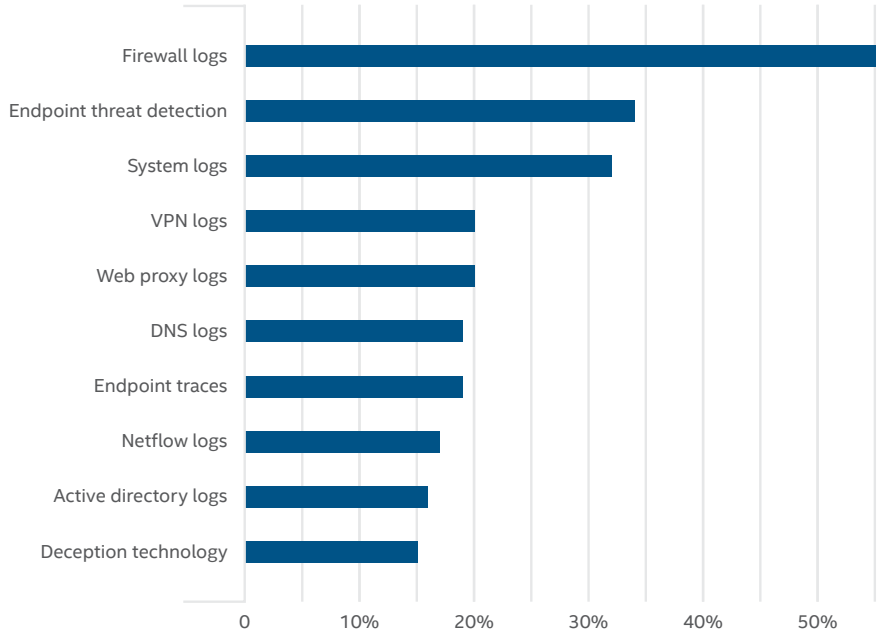


Source: Intel Security.

Sources of threat information

The majority of organizations (55%) reported that firewall logs are the primary source used for advanced threat detection and investigation, followed by endpoint logs (34%) and system logs (32%). Other data, such as logs from VPN activity, web proxies, DNS, and DHCP servers are used by 20% or less. Historical data, important for forensic investigations or historical correlation, is typically retained for between 45 and 60 days. Firewall logs, endpoint threat detection logs, and Active Directory logs are retained for the longest period.

What are the top 3 data sources used by your organization to detect advanced threats?



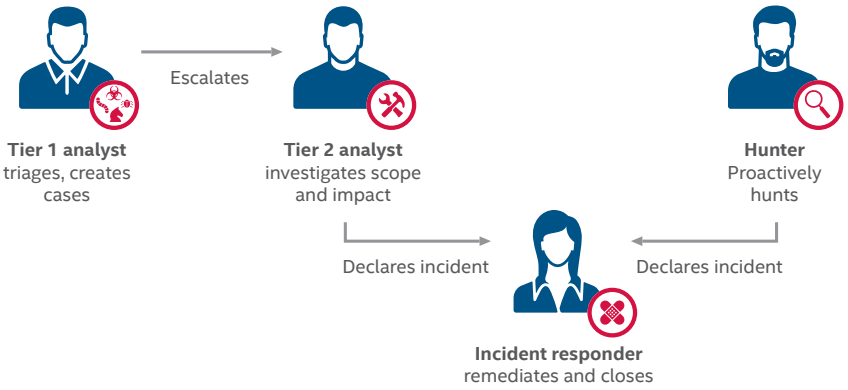
Source: Intel Security.

Staffing the SOC

Security professionals in this study were asked about four types of security teams:

- Tier 1 SOC analysts or equivalent. Triages, creates cases, prioritizes, and escalates.
- Tier 2 SOC analysts or equivalent. Investigates case scope and impact, can declare an incident.
- Hunter or equivalent. Proactively hunts for threats and can declare an incident.
- Incident responder or equivalent. Seeks to close threat incidents created by the SOC or hunter.

Security functions in the SOC



Source: Threat Management Platform Study, Intel Security research, July 2016.

Median internal staffing levels are 10 to 15 people for each team of Tier 1 SOC analysts, Tier 2 SOC analysts, hunters, and incident responders. Only 15% of organizations currently operate all four types of teams.

On average three of these teams are involved with investigating a case, scoping it and making a security decision, and responding to or remediating an incident. Median internal staffing levels are 10 to 15 people for each team of Tier 1 SOC analysts, Tier 2 SOC analysts, hunters, and incident responders, but only 15% of organizations currently operate all four types of teams. MSSPs are often asked to augment a team's skills and capacities, and contribute roughly one-third of total resources for each team. There is no significant variation in the percentage of external resources used by country or organization size. However, it is not surprising that larger organizations have larger teams. Although the median staffing level for Tier 1 teams is 15 people regardless of company size, Tier 2, hunter, and incident responder teams are about 50% larger in enterprises than in commercial organizations.

More than 65% of organizations with SOCs have formal threat-hunting operations, especially in large enterprise organizations, in which it was reported by almost 75% of those surveyed. Commercial organizations tend more toward an ad-hoc approach, with 41% of them using this less formal method. Only 5% of organizations report no active threat hunting. Formal threat hunting shows a strong relationship with SOC models and maturity levels. A bit more than 60% of organizations running virtual, co-managed, or multifunction SOCs have formal threat hunting, compared with more than 70% of those with dedicated or command SOCs.

Areas for growth

Security operations appear to be maturing, with sophisticated tools and well-staffed teams augmented by external resources. However, they are not keeping up with the volume of alerts and incidents, putting them at significant risk of a moderate or severe breach. What are their plans for enhancing their capabilities?

Most of these organizations consider themselves to be similar to their peers in information security investments and speed of adoption of new security capabilities. However, around 30% think that they are above average in investment or technology adoption, and only about 10% think they are below average.

The highest priority for future growth and investment is to improve the ability to respond to confirmed attacks, including coordination, remediation, eradication, and preventing reoccurrence. Methods to address this goal includes the three pillars of people, processes, and technology.

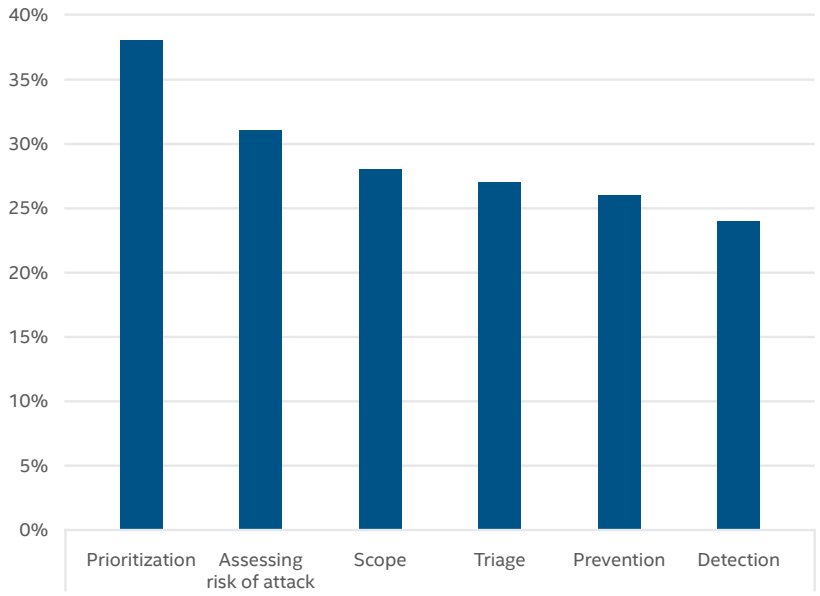
The priority areas for future growth and investment are, in order:

- Improve the ability to respond to confirmed attacks, including coordination, remediation, eradication, and preventing reoccurrence.
- Improve the ability to detect signals of potential attacks, including focusing on relevant events and alerts, triage, and prioritization.
- Improve the ability to investigate potential attacks, including scoping the full extent and impact of an attack.

Methods to address these goals include the three pillars of people, processes, and technology. Of the organizations that do not yet have all four types of security teams operating, 40% plan to deploy internal people into those roles within 12 to 18 months. Similarly, around 40% of organizations plan to increase their use of MSSP people within one or more of these security functions in that period. Deploying new security technology is another way to enhance capabilities, with more than 60% of organizations planning to invest in tools for these teams. Given the significant percentage of organizations that are not managing to triage and investigate all of their alerts, it is not surprising that key processes are the top two focus areas for new tools: improving the speed and accuracy of initial triage and prioritization of security alerts, and reducing the time and effort it takes to conduct incident investigations.

Security analytics is of growing interest to help address the volume of alerts, and is already in use by 67% of these organizations. Detection is reported as the number one purpose today for analytics, but prioritization and risk assessment are likely to be the top two drivers for future adoption of security analytics during the next 12 to 18 months.

What are the drivers of your company's adoption of security analytics solutions in the next 12–18 months?



Source: Intel Security.

Policies and procedures

Advancing the maturity level of a SOC involves three design principles. First, objectively evaluate the current level of organization maturity. What are the team's strengths and weaknesses, where are the gaps, and what is the risk posture? As part of this, identify the metrics necessary for ongoing evaluation, and the data necessary to calculate them.

To learn how Intel Security can help you optimize your security operations, click here.

Next, shift the emphasis to time to detection, containment, and remediation. These times are the most effective way to focus attention and resources where they are most needed. Reducing these security times usually requires a combination of integration, automation, and improving workflows. Anywhere that the number of process steps can be reduced, human interaction eliminated, or duplication removed should be priorities.

Finally, automate as many tasks as possible to augment limited human resources, improve accuracy by reducing human error, and broaden coverage of repeatable actions. Begin the automation process with low-risk tasks, and work up as confidence increases. It is important to first optimize processes and then automate to get the best results.

Conclusion

SOCs are back and continuing to expand
SOCs have returned from movie land and become critical components of an organization's security posture. Data breaches are on the rise, whether from increased attacks or better detection, and SOCs can help security teams triage alerts, respond to incidents, coordinate investigations, and proactively hunt for threats. There is no perfect SOC model. Whether the SOC is internal or external, dedicated or multifunction, the important thing is to continue improving security operations, from reactive to proactive and optimized.

Upgraded tools and capabilities still needed
Although SOCs have become more common, most organizations are still overwhelmed with alerts and are unable to properly investigate one out of four, resulting in minor or moderate business impacts. As a result, most feel it is important to continue making improvements to their internal security capabilities, continue or increase their use of MSSPs, and invest in additional or enhanced tools.

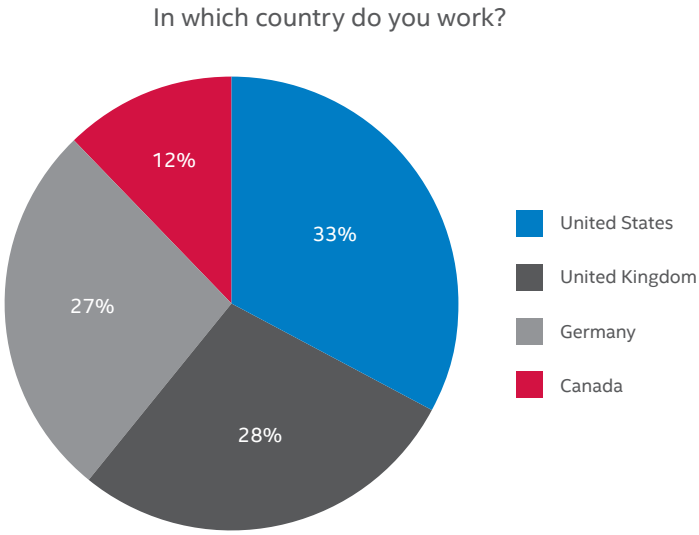
Three major investment priorities
During the next 12 to 18 months, organizations plan to invest in three major areas to improve their capabilities: responsiveness, detection, and investigation. Methods of improvement vary by country, organization size, and other attributes. These appear to be dependent on the availability of local resources, whether skilled security personnel, new and enhanced tools, or capable MSSPs.

To learn how Intel Security can help you optimize your security operations, click here.

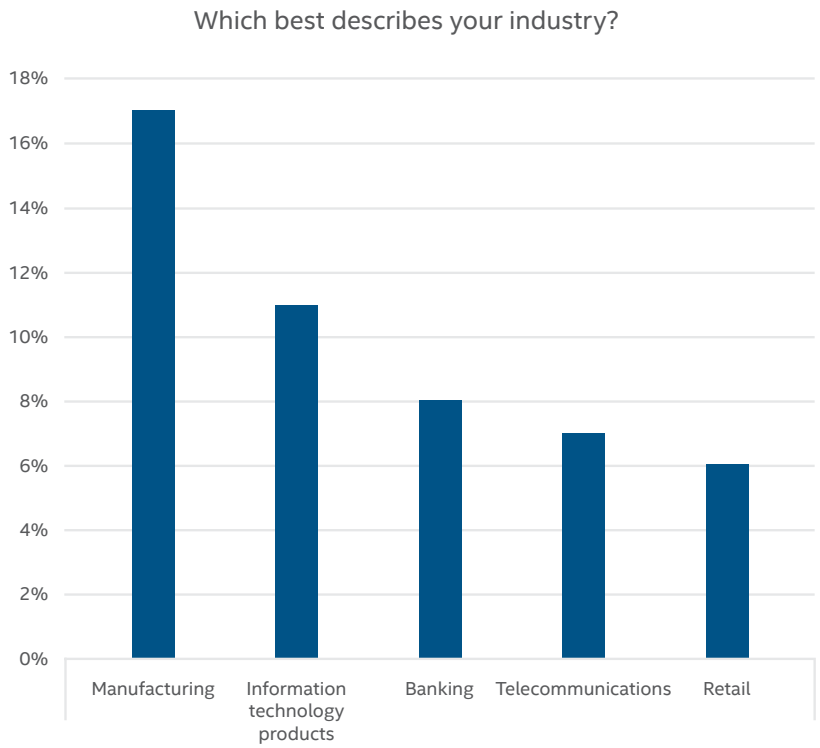
For more security operations reports and resources, click here.

Methodology

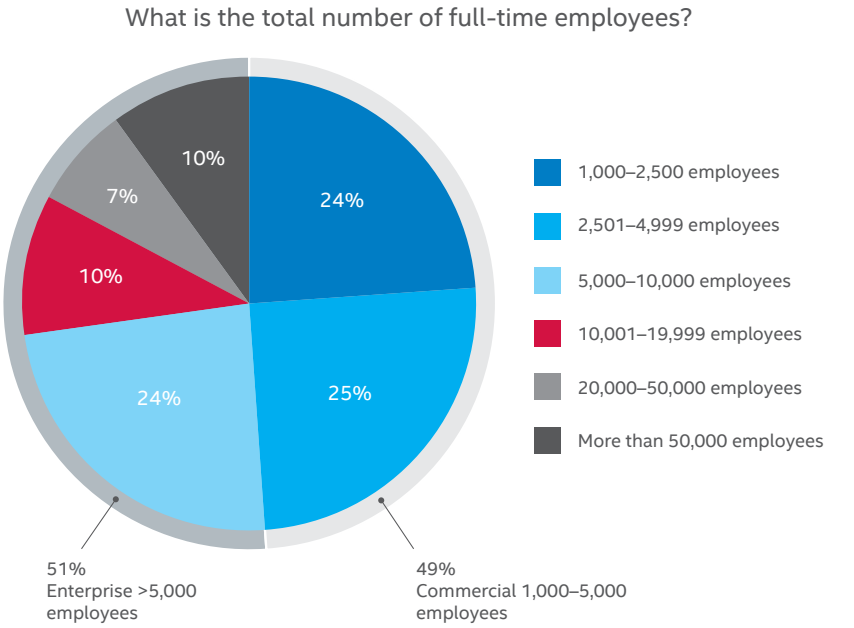
Intel Security surveyed a panel of 390 IT security decision makers from Canada, Germany, the United Kingdom, and the United States. Respondents covered a variety of organization sizes, industries, job titles, and employment tenure.



Source: Intel Security.



Source: Intel Security.



Source: Intel Security.

A year at ransom

—Christiaan Beek, Raj Samani, and Douglas Frosst

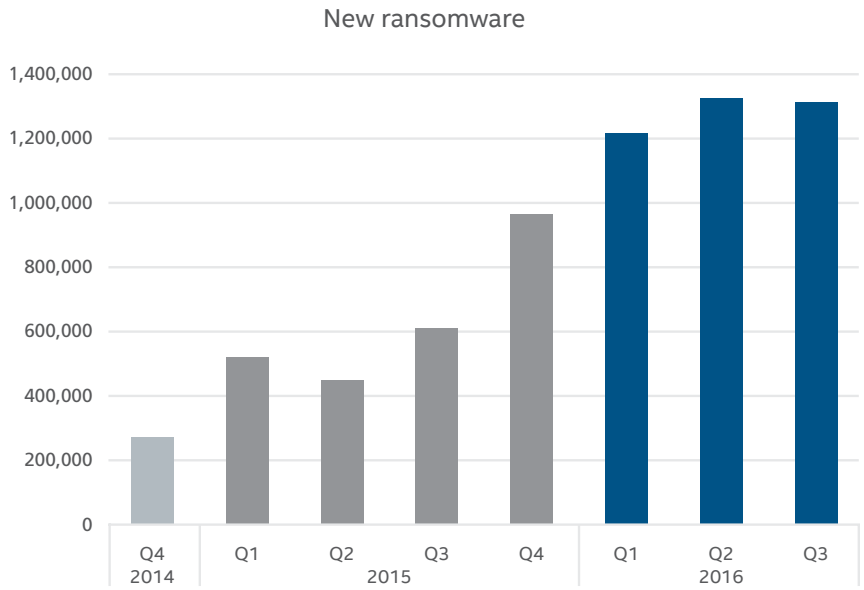
In the *McAfee Labs 2016 Threats Predictions report*, published last autumn, we claimed that 2015's spike in ransomware attacks would continue and that ransomware would be a major and rapidly growing threat in 2016. As predicted, 2016 may be remembered as "the year of ransomware," with both a huge jump in the number of ransomware attacks and significant technical advances in this type of attack.

A brief history of ransomware

Ransomware dates to 1989, when 20,000 infected floppy disks were distributed at the World Health Organization's AIDS conference. Using symmetric encryption, this attack was quickly broken. The first asymmetric encryption implemented in a cryptovirus attack was published in Adam Young's 1995 master's thesis: "Cryptovirology and the Dark Side of Black Box Cryptography." The size of the virus was a little less than 7KB. It was not until the mid-2000s that asymmetric encryption, which is much more difficult to decipher, was used in a ransomware attack.

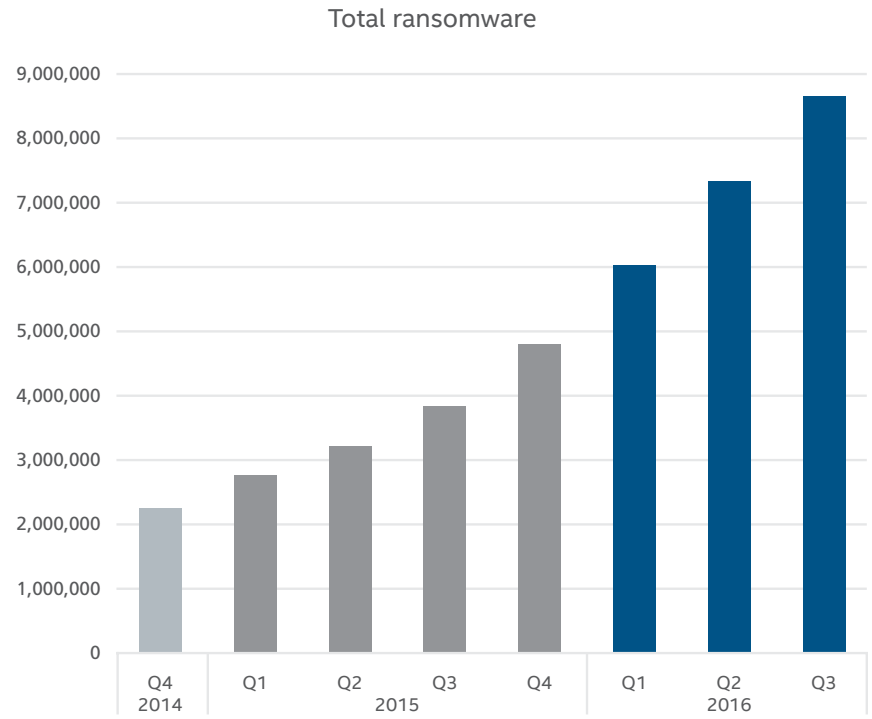
The emergence of Bitcoin enabled anonymous transactions and provided an important foundation for future growth in ransomware attacks. CryptoLocker established the modern ransomware era in 2013. Ransomware-as-a-service was introduced in 2015, making this type of attack available to almost anyone with a computer.

At the time, one of the big challenges for attackers was how to get paid without getting caught. They experimented with a variety of methods. The emergence of Bitcoin and similar digital currencies in 2009 enabled anonymous transactions and provided an important foundation for future growth in ransomware attacks. CryptoLocker established the modern ransomware era in 2013, incorporating delivery via compromised websites, email attachments, control servers and with Tor networks as an additional form of obfuscation. Other variants and copycats soon followed, including CryptoWall and CTB-Locker. Ransomware-as-a-service was introduced in 2015, making this type of attack available to almost anyone with a computer, with the developers getting a commission on every successful campaign. Later that year we also saw an increase in the threat of exposure of sensitive files and trashing the operating system, in addition to encrypting the victim's data.



Source: McAfee Labs.

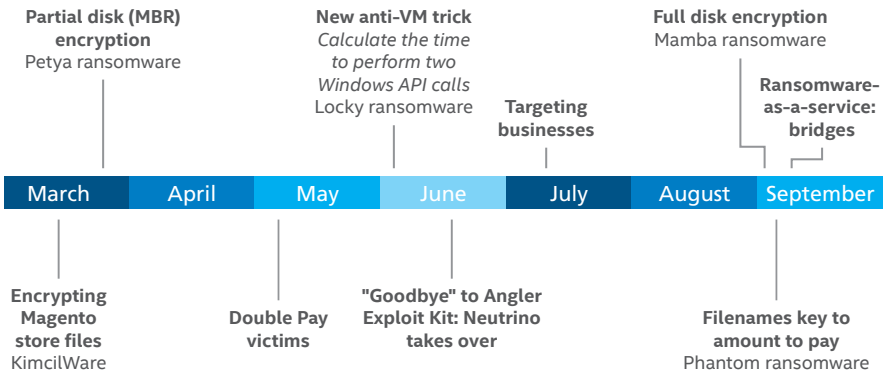
The count of total ransomware grew by 18% this quarter.



Source: McAfee Labs.

2016 ransomware timeline

This year, ransomware found a new and vulnerable target: hospitals. Although there was some criticism from the hacker community about these attacks, many of the victims paid, fueling further incidents. There was no real technical evolution in these attacks, just phishing emails targeting people using essential systems. However, the rest of the year saw considerable technical advances, including partial and full disk encryption, variable and increasing ransom demands, and new ransomware delivery mechanisms.



Source: McAfee Labs.

Partial disk encryption

In March we saw the appearance partial disk encryption instead of file encryption. This type of ransomware encrypts the master file table, making files inaccessible.

In March we saw the appearance of Petya and partial disk encryption instead of file encryption. This ransomware is often delivered via a fake job-applicant email with a Dropbox link, and begins the attack by overwriting the master boot record, rebooting, and executing the malware, putting up a fake CHKDSK screen that encrypts the master file table. While the files are still on the disk and unaffected, the encrypted file table prevents them from being located. Paying the ransom gets the decryption key, which unlocks the file table and boot record, and removes the malware boot loader.

Increasing ransom demands

Petya also brought on increasing ransom demands, doubling the amount if payment was not made within seven days. One ransomware variant threatened to delete one file per hour until the ransom was paid. Another encoded a series of ransom amounts, which it chose based on the name of the distribution file, making it quick and easy to make the demand fit the victim's ability to pay. In another case, a hospital that paid the first ransom demand was then told to pay again if it wanted to regain access to all of the files. The hospital ignored the second demand, but it remains an ongoing concern that attackers will not be "honorable" in their actions and refuse to release encryption keys even after receiving payment.

Encrypting websites

In March, the ransomware family KimcilWare appeared. The ransomware does not attack the victims' machines but instead targets websites that use Magento ecommerce store files. By encrypting the files with a Rijndael (AES) block cipher and appending the extension .kimcilware at the end of each file, the store's files become useless. The attacker can be contacted on a Hotmail account and after paying US$140 in Bitcoins, the attacker hands over a decryption key to the victim.

KimcilWare's possible author is also associated with another piece of ransomware that is based on the proof-of-concept ransomware code Hidden Tear. In 2016, we have seen many ransomware samples based on this proof of concept code. The following image illustrates the correlation between different ransomware families associated with this code:

Source: McAfee Labs.

Anti-sandbox techniques

The common "sandbox" method used to detect ransomware can now be detected and evaded by some ransomware.

Suspicious files are often sent to a "sandbox" for evaluation before being allowed to run on a user's system. This year, ransomware attackers learned how to differentiate between a sandbox, which is usually a virtual machine, and a live human's device. In a recent case, Locky, the culprit in many of the hospital ransomware attacks, used encrypted code and execution time differences between real and virtual machines to evade detection. Two API calls, *GetProcessHeap()* and *CloseHandle(),* one of which should be about 10 times faster on a real system, are run by the malware, which goes dormant if the execution time difference is not as large as expected.

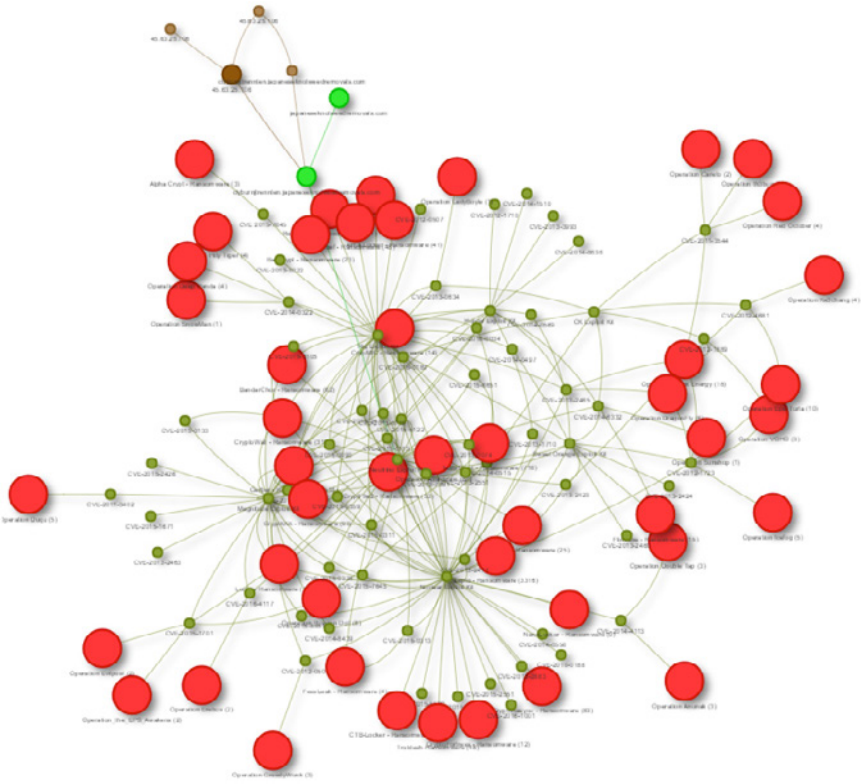
At the same time, the command-line argument "123" is used to execute the ransomware. Sandboxes in general execute the malware without any arguments. By not having the right argument, the ransomware will terminate and cannot be fully analyzed by the sandbox technology.

Another new anti-sandbox technique looks at Microsoft Office's recent files collection. If the number of files in this list is very small, it assumes that it is in a virtual machine and shuts down. Or the ownership of the IP address is checked against a list of known security vendors and cloud security providers.

Goodbye Angler, hello Neutrino

In 2015 and the first half of 2016, the Angler exploit kit was the most popular mechanism for delivering ransomware to potential victims. These exploit kits are popular and have a strong support system. However, in April and May, the volume of Angler traffic dropped dramatically, eventually shutting down completely. It appeared to have been replaced in popularity by Neutrino, although at nowhere near Angler's volume of traffic. Another shift in exploit kits happened in September, with RIG rising to challenge Neutrino for top spot. Whatever is driving these changes in the ransomware delivery marketplace, expect continued variations as attackers look for new ways to evade defenses.

We track the use of exploit kits in different campaigns and the vulnerabilities they exploit. By knowing which exploits are used, we inform our customers which patches they should prioritize to assist them in reducing their vulnerability to these attacks. Correlating our research with third-party data sources results in the following example:



Source: McAfee Labs.

In the preceding picture, the red dots represent campaigns to which we can attribute the use of the Neutrino exploit kit. A few examples of these ransomware campaigns:

- Locky
- Cerber
- CryptXXX
- PizzaCrypts
- Zepto

Targeting businesses

There has been a significant shift by ransomware attackers to business targets, as a few successful campaigns have encouraged more attacks.

Generally speaking, ransomware attacks began in the 1990s as seemingly random campaigns, with broad delivery mechanisms used to catch the occasional consumer. In the past year, we have seen a significant shift to business targets, as a few successful campaigns have encouraged more attacks. Typical targets include essential services such as hospitals, but also small and medium-sized businesses, which often lack a fully staffed cybersecurity operation. The initial attack vector for many of these campaigns is targeted phishing emails aimed at a specific individual or job function. In addition to encrypting files, the malware captures user credentials to steal data or spread the infection throughout the organization.

Full disk encryption

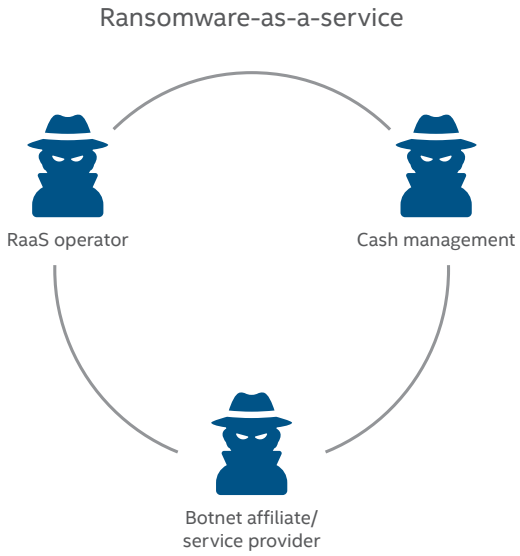
New ransomware variants encrypt complete disk partitions.

While Petya encrypts the boot record and file table, the Mamba ransomware encrypts complete disk partitions. The code responsible for the full disk encryption is not homemade but borrowed from the tool DiskCryptor. Not only does this encryption make a partition's files inaccessible, it also prevents the operating system from booting, requiring victims to use another machine to contact the attacker for payment and recovery instructions. Mamba also adapted the previously described anti–virtual machine technique, using a password as a command-line argument to execute the malware.

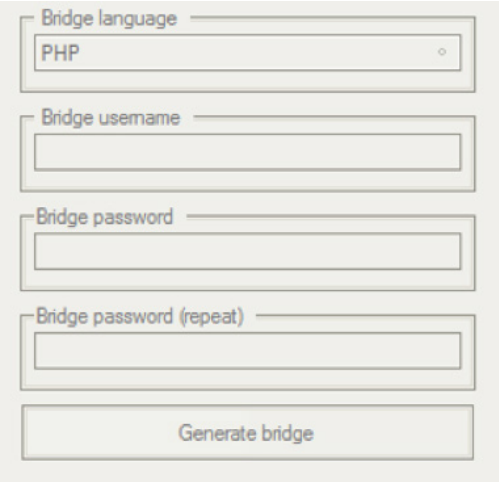
Ransomware-as-a-service

"Ransomware-as-a-service" has emerged: Attackers buy access to a ransomware service and pay a percentage of their campaigns' revenue to the service provider.

When cybercriminals do not have technical skills, infrastructure, or time, they can now participate and set up their own ransomware campaigns and extort money from victims within hours. This is the aim of "ransomware-as-a-service." The infrastructure is set up by a criminal service provider. Attackers buy access to it and pay a percentage of their campaigns' revenue to the service provider.



Ransomware-as-a-service providers recently introduced the concept of bridges, which are PHP scripts that connect attackers with their victims. The script uses itself as a database and stores client keys, operating systems, IP addresses, and ransom amounts, verifies the status of payments and delivers victims' information to the main servers. Bridges are password protected and avoid detection by search engines.



Not all bad news

This summer, a group of security vendors and law enforcement organizations, led by Europol and including Intel Security, announced the "No More Ransom!" collaboration to fight ransomware. This effort includes prevention advice, investigation assistance, and decryption tools.

This year has not been solely one of victories for cybercriminals; there were some notable advances on the defensive front as well, including several takedowns, keys recovered, and the advent of an anti-ransomware alliance.

No More Ransom!
In July, a group of security vendors and law enforcement organizations, led by Europol and including Intel Security, announced their collaboration to fight ransomware. This effort includes prevention advice, investigation assistance, and decryption tools. The No More Ransom! website provides a wealth of information on ransomware, including direct links to tools for decrypting files using recovered keys.

On the No More Ransom! site, decryption tools are available for Chimera, Coinvault, Marsjoke, Rakhni, Rannoh, Shade, Teslacrypt, and WildFire ransomware. New tools are developed and made available at No More Ransom! as ransomware is reverse engineered or encryption keys recovered during takedowns of ransomware control servers.

Originally a collaboration of four organizations, this initiative has since added 13 new law enforcement partners in Bosnia and Herzegovina, Bulgaria, Colombia, France, Hungary, Ireland, Italy, Latvia, Lithuania, Portugal, Spain, Switzerland, and the United Kingdom. No More Ransom! has allowed ransomware victims to avoid paying an estimated US$1.48 million (€1.35 million) in ransom payments to cybercriminals. The No More Ransom! portal has received more than 24.5 million visitors since its launch, for an average of 400,000 visitors per day.

Takedowns
There have been several takedowns of ransomware systems this year, with more in process. Two major ones efforts this year were Shade in July and WildFire in September. Law enforcement and security vendors continue to collaborate on these threats, sharing threat intelligence, research, and recovery efforts.

Policies and procedures

The most important step to protect systems from ransomware is to be aware of the problem and the ways in which it spreads. Here are a number of policies and procedures businesses should follow to minimize the success of ransomware attacks:

- Have a plan of action in the event of an attack. Know where critical data is located and understand if there is a method to infiltrate it. Perform business continuity and disaster recovery drills with the emergency management team to validate recovery point and time objectives. These exercises can uncover hidden impacts to business operations that do not otherwise surface during normal backup testing.
- Keep system patches up to date. Many vulnerabilities commonly abused by ransomware can be patched. Keep up to date with patches to operating systems, Java, Adobe Reader, Flash, and applications. Have a patching procedure in place and verify if the patches have been applied successfully.

To learn how Intel Security products can help protect against ransomware, click here.

- For legacy systems and devices that cannot be patched, mitigate the risk by leveraging application whitelisting, which locks systems and prevents unapproved program execution. Segment these systems and devices from other parts of the network using a firewall or intrusion prevention system. Disable unnecessary services or ports on these systems to reduce exposure to possible entry points of infection.
- Protect endpoints. Use endpoint protection and its advanced features. In many cases, the client is installed with only default features enabled. By implementing some advanced features—for example, "block executable from being run from Temp folder"—more malware can be detected and blocked.
- If possible, prevent the storage of sensitive data on local disks. Require users to store data on secure network drives. This will limit downtime because infected systems can simply be reimaged.
- Employ an antispam tool. Most ransomware campaigns start with a phishing email that contains a link or a certain type of attachment. In phishing campaigns that pack the ransomware in a .scr file or some other uncommon format, it is easy to set up a spam rule to block these attachments. If .zip files are allowed to pass, scan at least two levels into the .zip file for possible malicious content.
- Block unwanted or unneeded programs and traffic. If there is no need for Tor, block the application and its traffic on the network. Blocking Tor will often stop the ransomware from getting its public RSA key from the control server, thereby blocking the ransomware encryption process.
- Add network segmentation for critical devices.
- "Air gap" backups. Ensure backup systems, storage, and tapes are in a location not generally accessible by systems in production networks. If payloads from ransomware attacks spread laterally, they could potentially affect backed-up data.
- Leverage a virtual infrastructure for critical systems that are air gapped from the rest of the production network.
- Perform ongoing user-awareness education. Because most ransomware attacks begin with phishing emails, user awareness is critically important. For every 10 emails sent by attackers, statistics have shown that at least one will be successful. Do not open emails or attachments from unverified or unknown senders.

To learn how Intel Security products can help protect against ransomware, click here.

"Trojanized" legitimate software is on the rise

—Craig Schmugar

Earlier this year, the Internet blew up over the topic of whether Apple should assist the FBI by providing access to a deceased terrorist's iPhone. Tim Cook, Apple's chief executive, referred to government's demands as asking for the "equivalent of a master key, capable of opening hundreds of millions of locks." In the end, the FBI gained access through undisclosed means and withdrew the request, but the notion of backdoor access is something that has been coveted by malware authors, spies, and nation-states for decades. Tactics for accomplishing this goal range from persuading victims via social engineering to hand over the keys to their devices, to intercepting hardware in the supply chain and inserting backdoors to surreptitiously gain remote access. However, the most common method is through the deployment of Trojan software.

We see a trend toward "Trojanizing" legitimate applications, which are injected with malicious nonreplicating code.

Most malicious applications today are rotten to the core. They serve one purpose, to profit bad actors, subjecting their victims to attacks. The tactical objectives of such crimes are generally to reach the target, establish a presence, and persist for an extended time. To reach their targets, attackers either draw victims in through social engineering or intercept their everyday computer usage, most often through exploitation. In either case, the goal is for those unfortunate enough to cross paths with malicious code to be none the wiser. The longer attacks can go unnoticed, the larger the payout. To this end, attackers are growing more sophisticated as they endeavor to create long lasting, fully undetectable creations. The more authentic-looking a piece of code, the more likely it is to be overlooked. This is the primary driving factor in an increasing trend of "Trojanizing" legitimate applications, which are injected with malicious nonreplicating code.

Attacker benefits

The abuse of reputable applications affords attackers a number of benefits. Payloads are concealed behind a recognizable brand, contributing to the impression of legitimacy and helping ensure targeted users take the bait. This brand recognition continues after a system has been compromised, through recognizable directory, file, process, and registry key names and attributes. These elements can provide cover during security scans and forensics analysis, with recognizable properties blending with hundreds or even thousands of familiar programs.

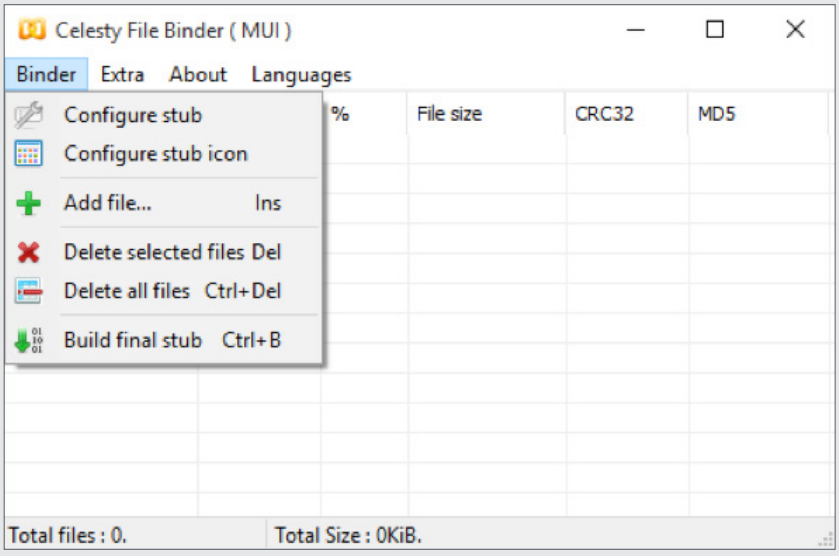
Another benefit is built-in persistence, or a method of restarting code that was previously terminated. Malware persistence falls into one of two categories: self-persistence, involving the installation of start-up hooks to endure reboots; and companion-persistence, which leverages existing start-up hooks to automatically load before, during, or after other wanted applications. Each system change made by malicious code is an indicator of compromise. Thus the fewer the number of changes, the smaller the detection surface. Trojanizing legitimate applications provides free persistence; the software's natural method of start-up is all that is necessary for the malicious code to load. In fact, if the program is run manually on a regular basis, then persistence is self-perpetuated by the victims themselves.

Methods of illegitimacy

The idea of riding on the coattails of popular applications harkens to the early days of malware creation, arguably with the inception decades ago of the very first parasitic file-infecting virus. Viruses differ from Trojans in that they recursively self-replicate, meaning that they spread to other files, those files in turn spread to other files, and so on. Part of the threat is the replication logic, which decides the files to target and where to insert malicious routines. Viruses can be analyzed and reverse engineered, and the replication logic and markers provide an additional detection surface for antivirus software. Parasitic Trojans, on the other hand, do not self-replicate, allowing for inserted code to be streamlined toward the desired payload without the additional overhead and corresponding detection surface. This can be an Achilles heel for defenses that are ill equipped to cope with such attacks.

Binders/Joiners

Binder programs first appeared in the 1990s and give malware distributors a quick and easy way to bundle their threats with other programs, documents, and multimedia files. Decoupling the malicious code from any social engineering aspects of an attack affords the perpetrators the benefit of customizing each binary for a given campaign, without having to code or recompile a threat. All that is required to build a new customized threat is to select current malware and accompanying files. The binder will combine all of them into a new executable ready for distribution. When a victim runs the program, both the malware and combined file will be run. Although binders do bundle clean and dirty files together, the result is a new piece of malware, which does not closely resemble a legitimate file.



The Celesty File Binder remains one of the most common binder programs in use.

Binding a clean application to a dirty one may provide some cover for those aiming to dupe users, but poisoning the master source code does a far better job. And when redistributed libraries are involved, this can result in other trusted software vendors perpetuating the erroneous trust.

Hacking the Source

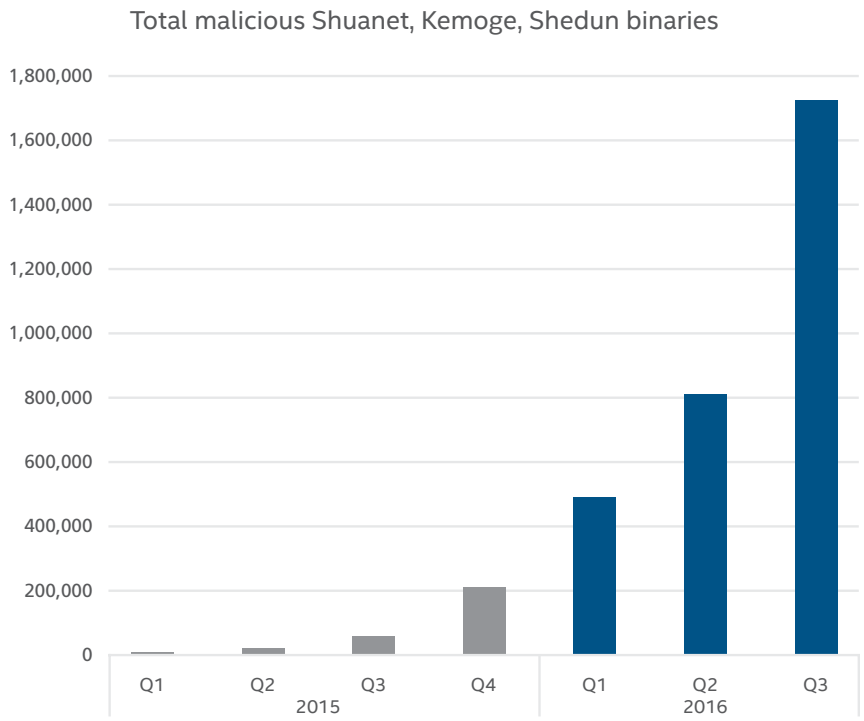
While binding a clean application to a dirty one may provide some cover for those aiming to dupe users, poisoning the master source code does a far better job. With the ability to add or modify code and configurations, or build scripts, attackers can impersonate software vendors and inherit the trust they have with their customers. Download servers, code signing, and all of the tenants of customer-facing authenticity are inherently present once the nefarious code has been successfully planted. And when redistributed libraries are involved, this can result in other trusted software vendors perpetuating the erroneous trust. Such was the case last year, when it was reported that the mobiSage software development kit contained a "backdoored" ad library that was subsequently consumed by thousands of iOS applications, including those distributed via the Apple App Store.

However, penetrating the internal source control server or build system of an organization that produces widely distributed software is generally wrought with challenges. Although instances of this have been made public in the past and are likely to continue in the future, this route is definitely not the path of least resistance.

The rapid growth of Android malware can be attributed to the modification of source code.

Modifying a copy of the source code is much simpler to do, especially with interpreted, open source, or decompiled code. Adding or modifying routines here is straightforward for anyone comfortable coding in the relevant programming language.

This ease is a prime factor in the rapid growth of Android malware, for which the creation of copycat apps is a regular occurrence. Last year, Lookout reported Trojanized adware masquerading as 20,000 popular apps. Our data shows this number has ballooned to nearly 700,000 in less than a year.



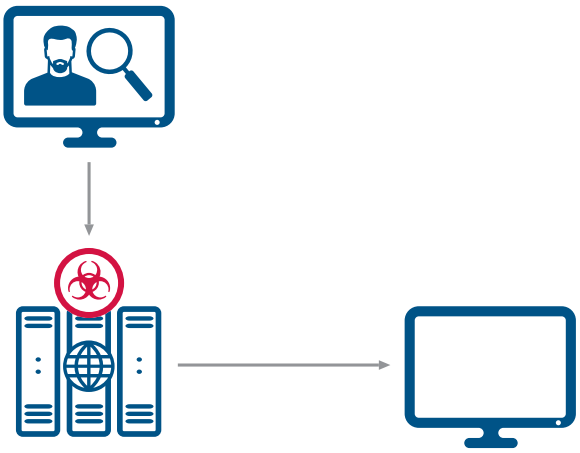
Source: McAfee Labs.

What about binaries for which the source is not available, or hackers unfamiliar with programming in the requisite language?

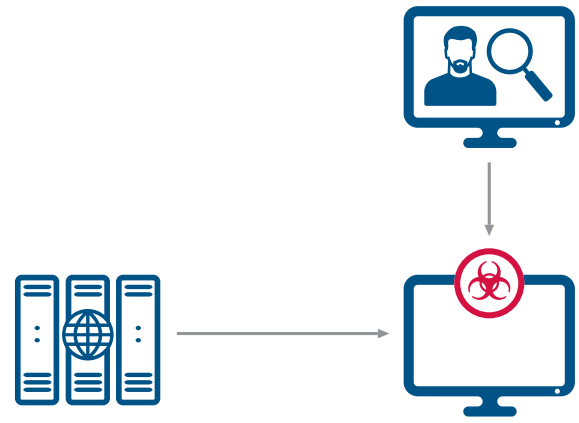
Binary patching programs have emerged in the last couple of years to simplify the process of adding malware payloads to already compiled applications.

Patchers

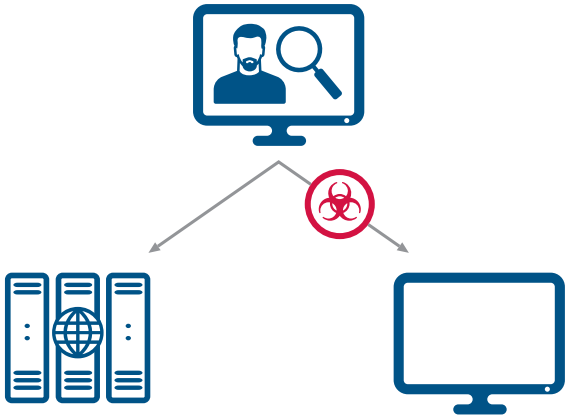
Binary patching programs have emerged in the last couple of years to simplify the process of adding payloads to already compiled applications. Unlike binders, patchers modify executables rather than create new ones. Payloads are strategically inserted with the goal of seamlessly maintaining application usage. These tools can be used in three scenarios: attacker/server side, client side, or man in the middle.



Attacker- or server-side patching. Tools run locally or remotely to statically patch binaries, which can be used to replace their desired counterparts.

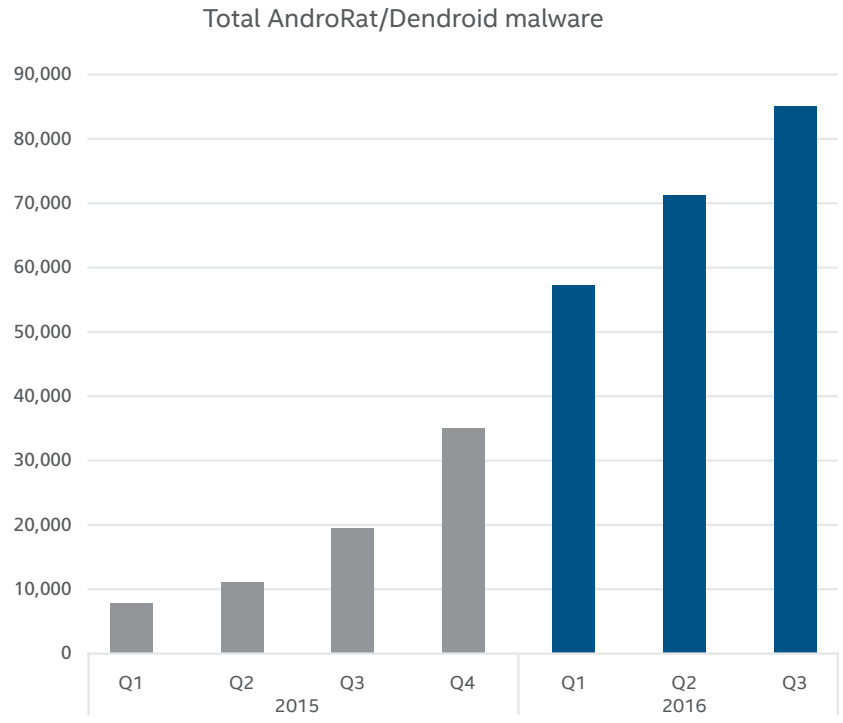


Client-side patching. Similarly, tools can run on the endpoint to patch local files.



Man-in-the-middle patching. A proxy server modifies binaries between the original source and the final destination.

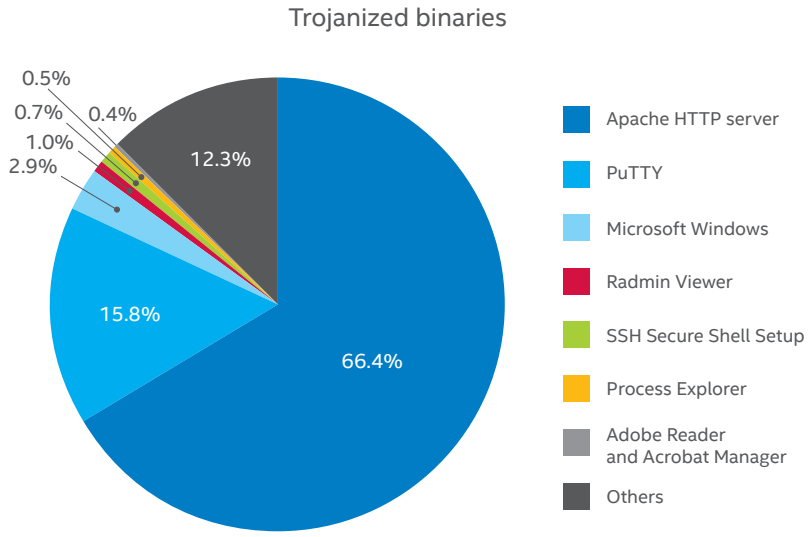
Regardless of the distribution approach, the binaries are modified to take the place of desired or known applications. Binary patching is perhaps most heavily used today in the realm of Android apps. Kits such as AndroRat and Dendroid are responsible for tens of thousands of copycat apps concealing malicious payloads.



Malicious Android binaries patched with popular backdoor kits.

Source: McAfee Labs.

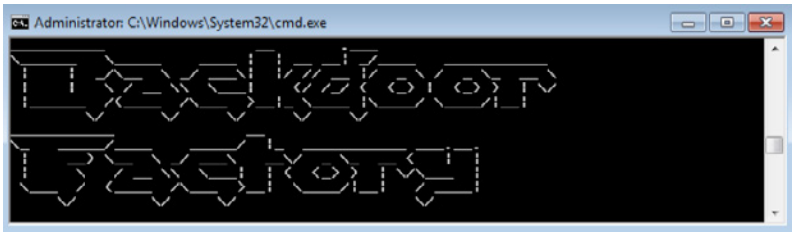
BackDoor Factory (BDF) is a popular open-source executable binary patcher that supports Windows, Mac, and Linux binary patching. Target programs are modified to include predefined or user-specified shellcode. BDF allows the operator to specify many options, including the host IP, port, and where to insert the shellcode within the target. Code can be placed in the slack space of a program and spread over one or more cavities, thus maintaining the original file size and executable geometry. This tactic may render certain feature vectors ineffective in machine learning algorithms applied to such threats.



Distribution of 29,000 Trojanized Windows binaries discovered in the past two years.

Source: McAfee Labs.

A BDF-patched PuTTY binary with payload split across multiple cavities.



The Backdoor Factory Proxy (BDFProxy) takes BDF a step further by patching executables on the fly as they are downloaded, leveraging a man-in-the-middle attack posture. Joshua Pitts, the author of the BDF tools, discovered this approach was actively being used in the wild in 2014 when applications were downloaded via a Tor exit node in Russia. This discovery was made within about an hour after the beginning of his search. In particular, all uncompressed Windows executable files served over nonsecured HTTP connections were modified to include the OnionDuke malware.

Who is at risk?

These attack scenarios apply to the majority of Internet users. Even those who seldom install new applications are likely to have existing applications configured for autoupdates. It is still commonplace for update servers to deliver binaries over insecure HTTP connections. Connecting to open Wi-Fi hotspots provides others an opportunity to carry out man-in-the-middle attacks. Running untrusted programs remains a significant attack vector, and the ever-growing use of shared libraries increases the overall risk, especially as it pertains to mobile devices and the Internet of Things.

Recommended policies and procedures

A VPN should be used when connecting to an untrusted network. Administrators should keep security software up to date and rely on strong indicators of trust rather than those potentially forged in an attack. Applications should be signed and verified with a chain of trust. Forensic analysis should include correlating hashes with trusted sources.

Security software should include dynamic analysis to flag rogue actions regardless of initial binary inspection because static scanning goes only so far. Behavioral monitoring, web and IP reputation, memory scanning, and application containment are welcome components in a complete solution.

Vendor downloads should occur over secure connections and all code should be signed. This drastically reduces man-in-the-middle attacks. Software vendors should include self-validation in their applications, regularly audit their code, use static code analysis tools, and perform peer reviews.

To learn how Intel Security products can help protect against Trojanized legitimate software, click here.

Summary

The problem of Trojanized legitimate applications is likely to get worse before it gets better. Research and development advancements in penetration testing and vulnerability assessment make it easier to both discover vulnerable applications and systems, as well as exploit them. We have seen how such tools are combined and improved. Defenses must evolve similarly to overcome this increasing threat.

To learn how Intel Security products can help protect against Trojanized legitimate software, click here.

Threats Statistics

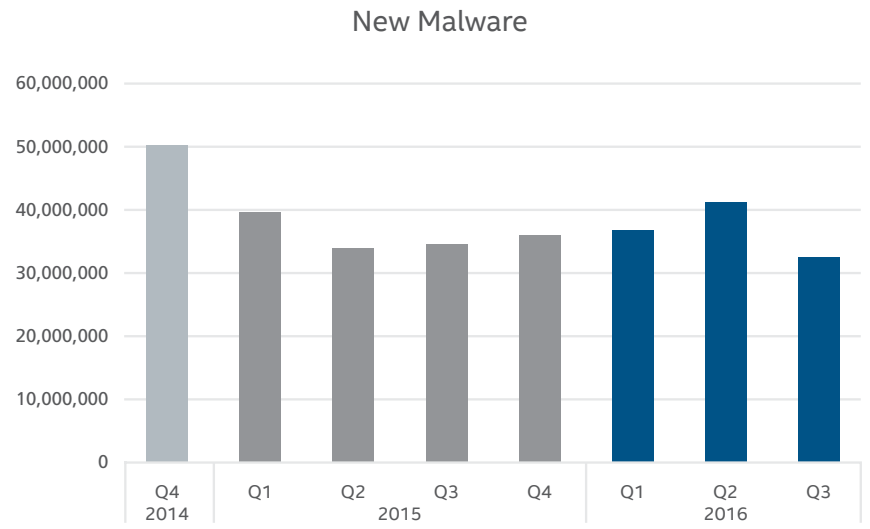
Malware

Web Threats

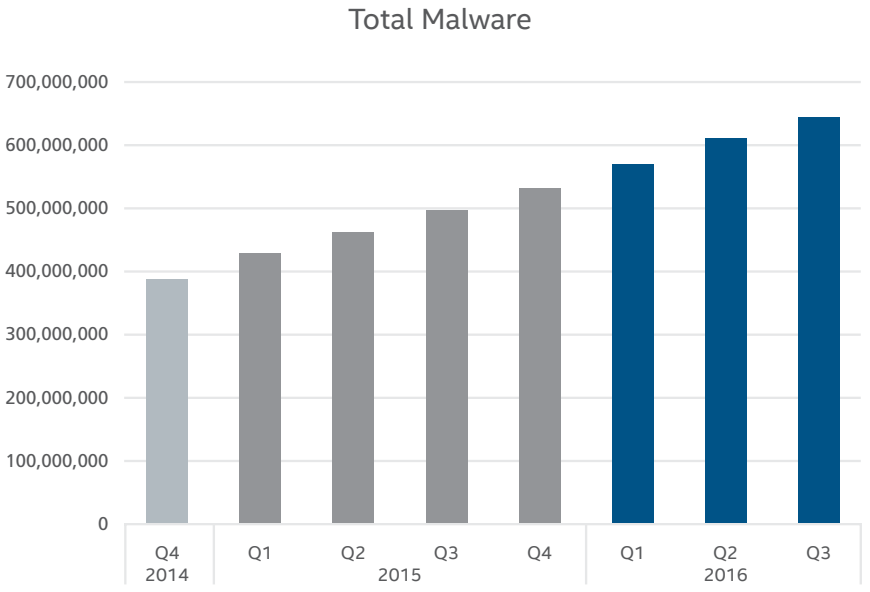
Share feedback

Malware

The growth of new unique malware dropped 21% in Q3.



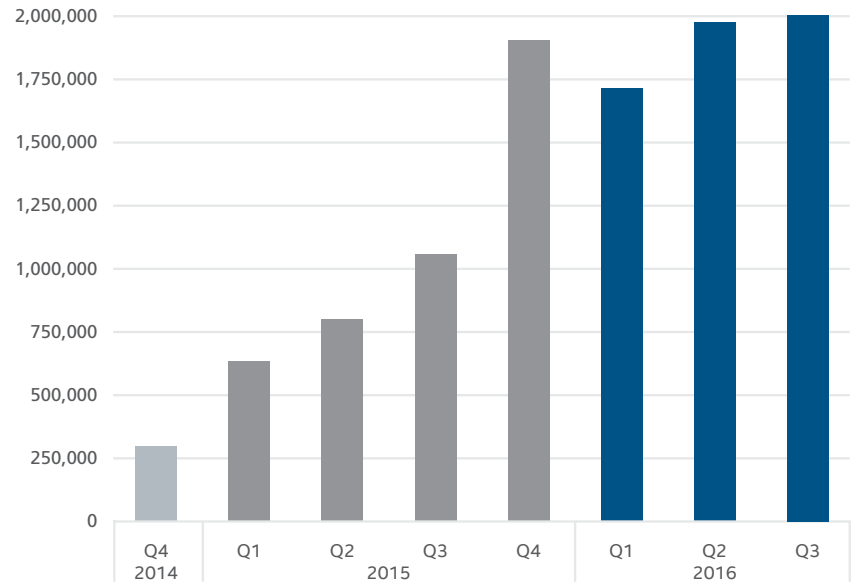
Source: McAfee Labs, 2016.



Source: McAfee Labs, 2016.

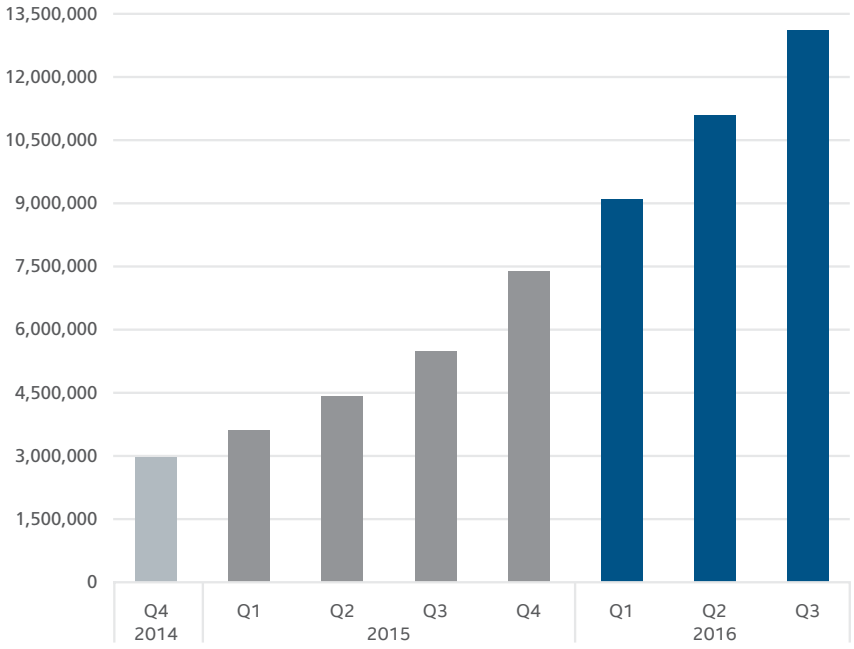
We cataloged more than two million new mobile malware threats in Q3.

New Mobile Malware



Source: McAfee Labs, 2016.

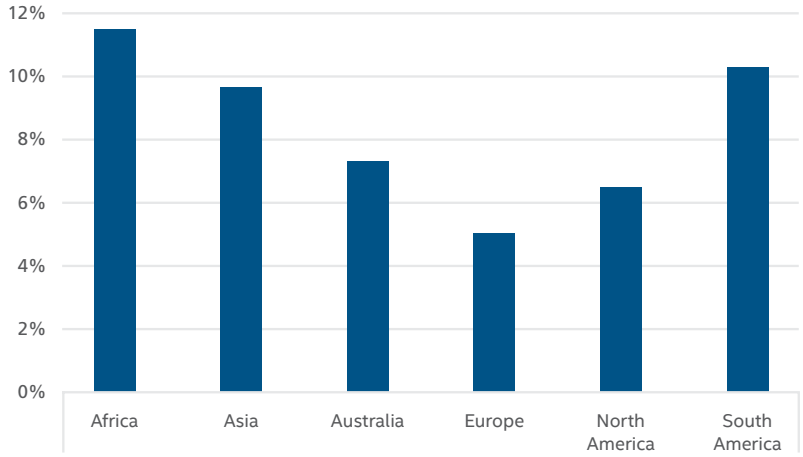
Total Mobile Malware



Source: McAfee Labs, 2016.

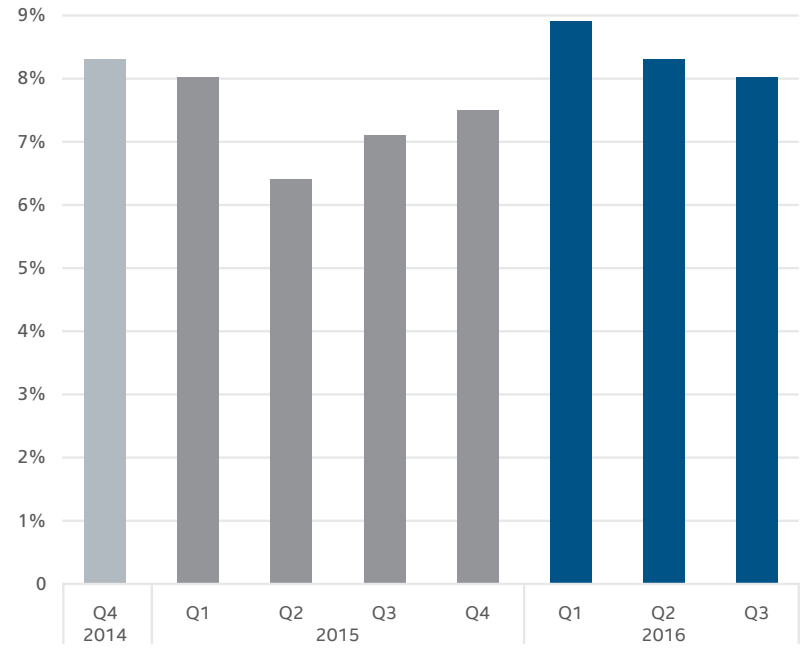
Infection rates in Africa and Asia each dropped by 1.5%, while Australia increased by 2% in Q3.

Regional Mobile Malware Infection Rates in Q3 2016
(percentage of mobile customers reporting infections)



Source: McAfee Labs, 2016.

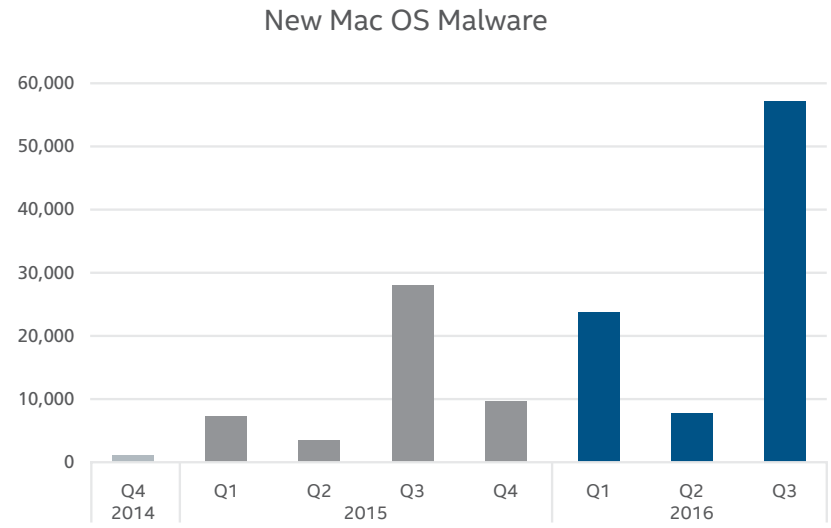
Global Mobile Malware Infection Rates
(percentage of mobile customers reporting infections)



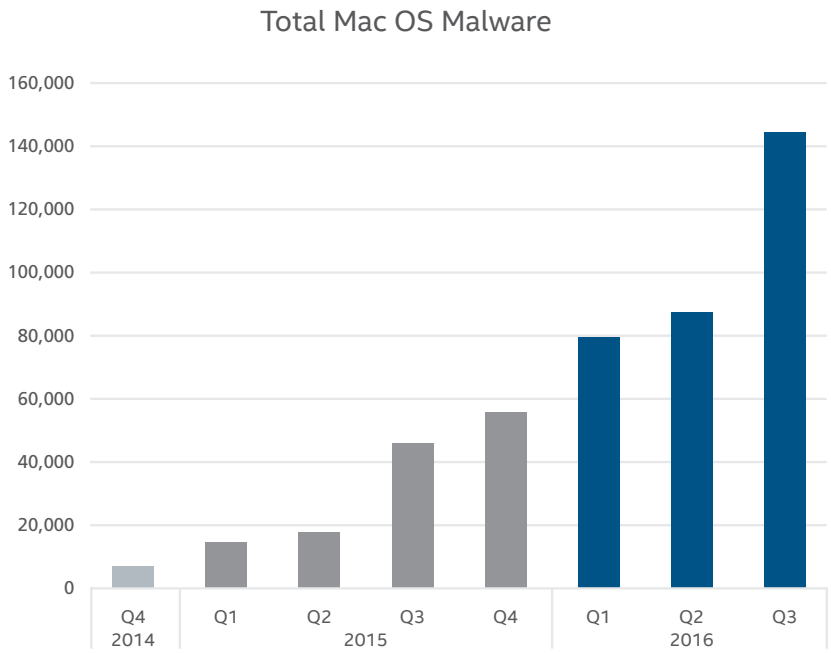
Source: McAfee Labs, 2016.

Share this Report

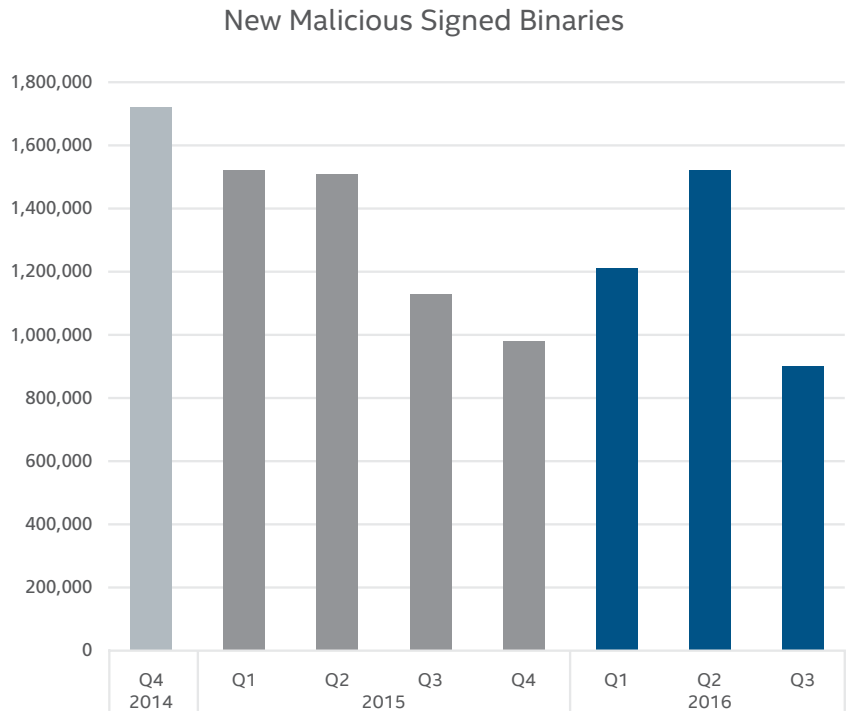
New Mac OS malware skyrocketed by 637% in Q3, but the increase was due primarily to a single adware family, Bundlore.



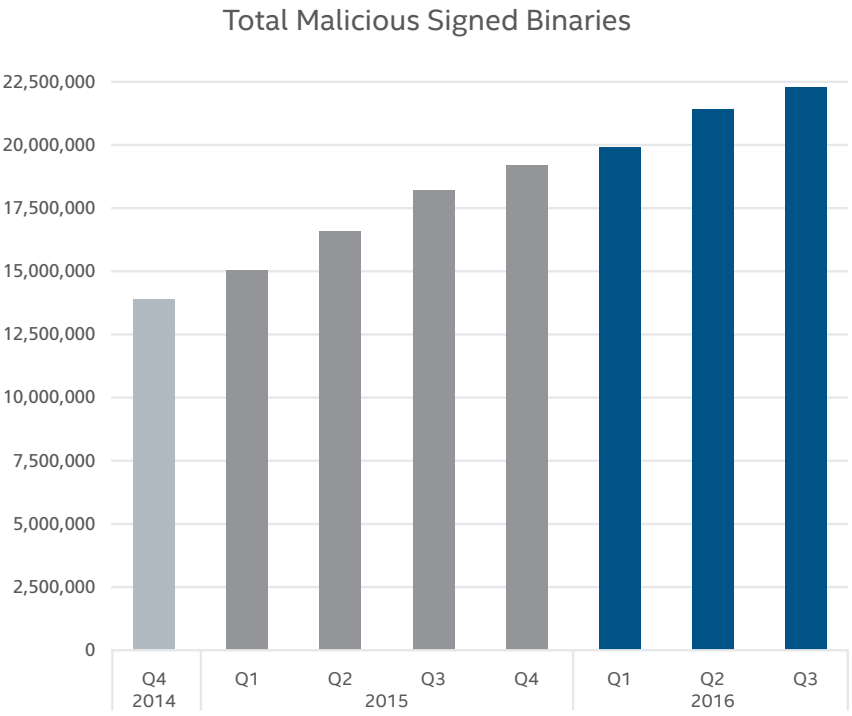
Source: McAfee Labs, 2016.



Source: McAfee Labs, 2016.

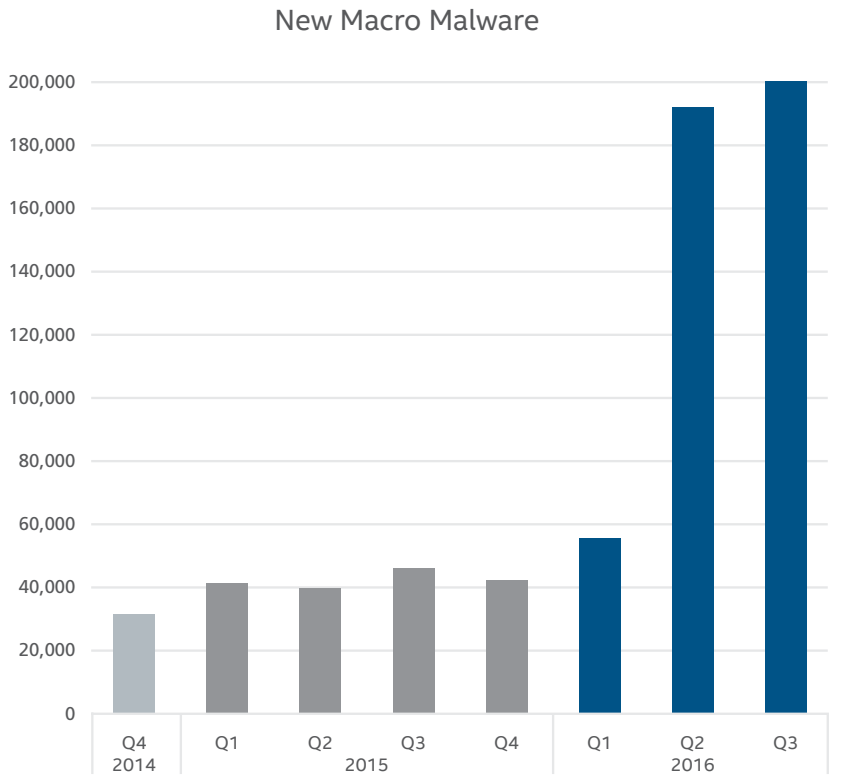


Source: McAfee Labs, 2016.

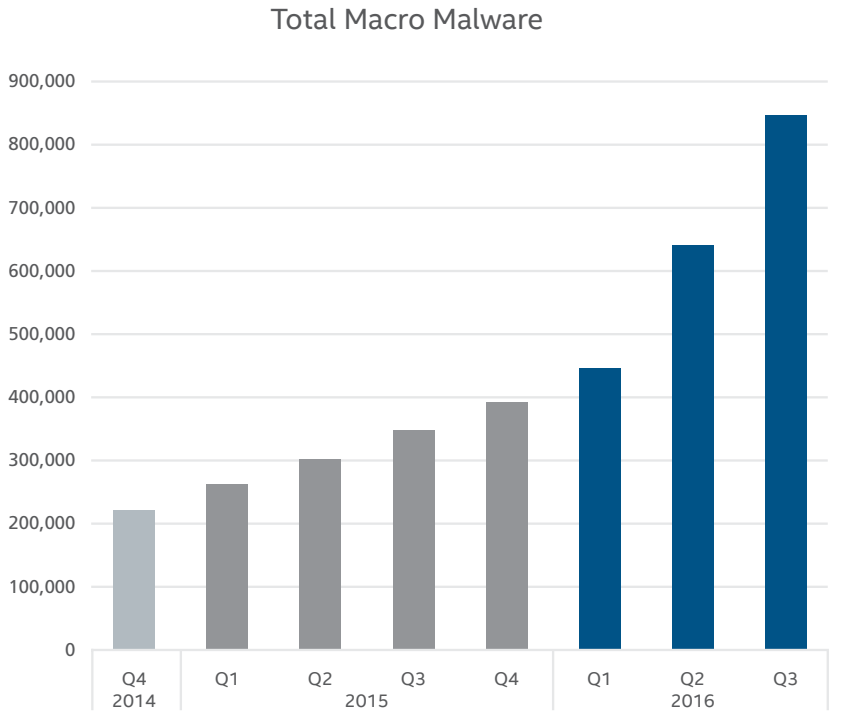


Source: McAfee Labs, 2016.

New Microsoft Office (primarily Word) macro malware continued the increase first seen in Q2.



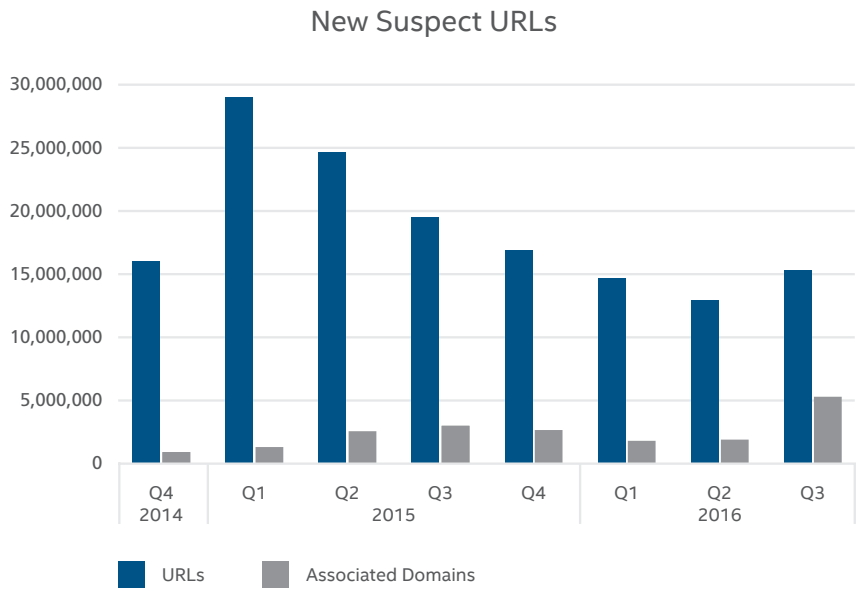
Source: McAfee Labs, 2016.



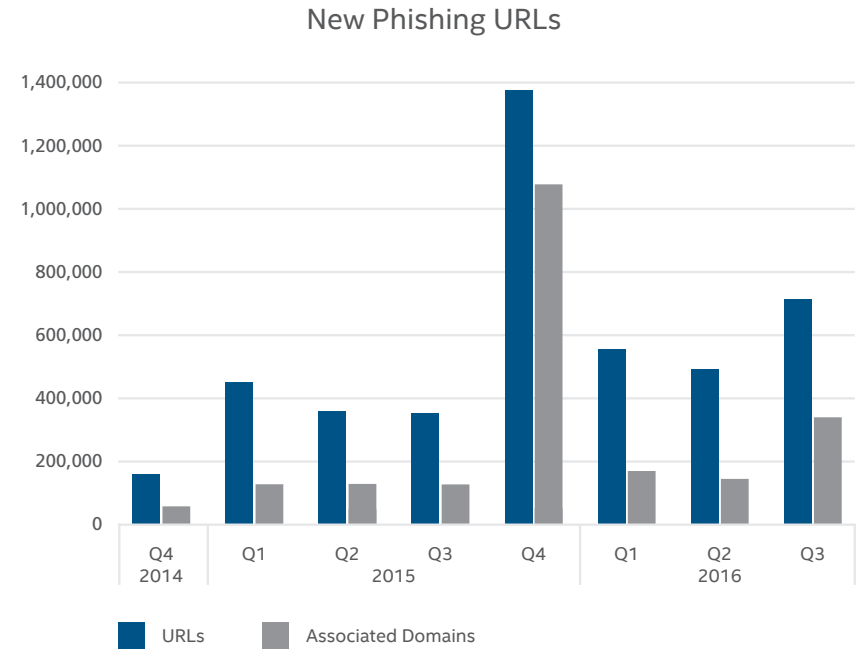
Source: McAfee Labs, 2016.

Share this Report

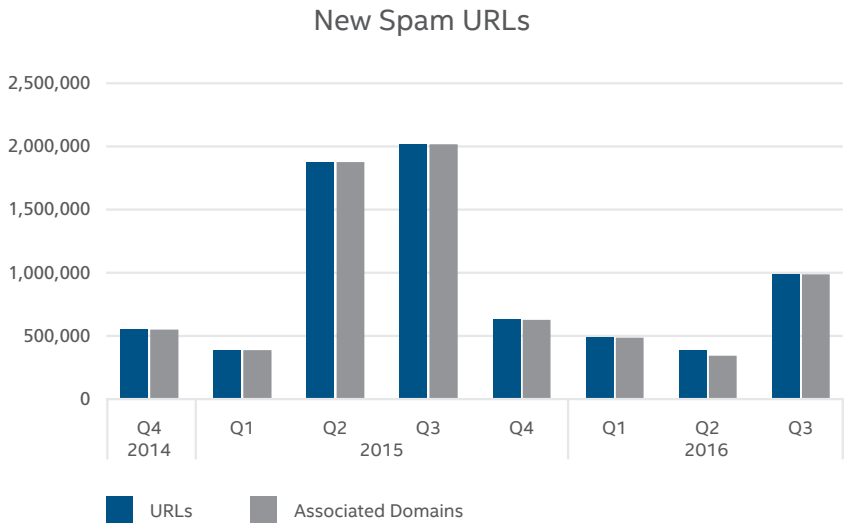
Web Threats



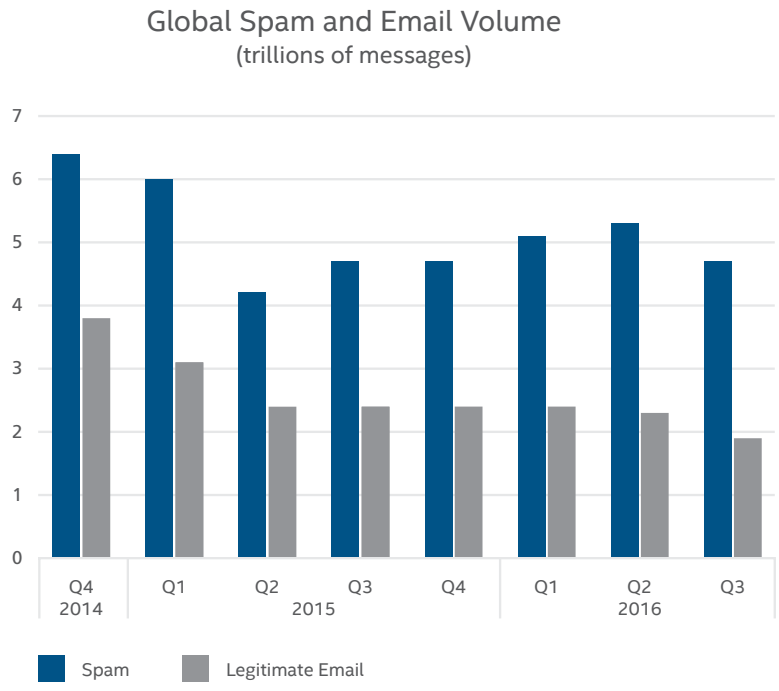
Source: McAfee Labs, 2016.



Source: McAfee Labs, 2016.



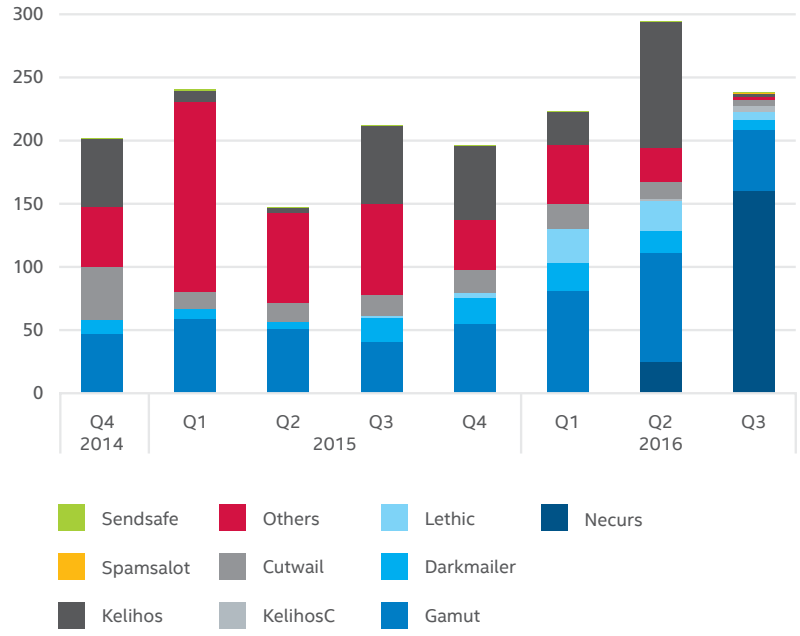
Source: McAfee Labs, 2016.



Source: McAfee Labs, 2016.

The Necurs botnet multiplied its Q2 volume by nearly seven times, becoming highest-volume spam botnet of Q3. We also measured a sharp drop in spamming by Kelihos, which resulted in the first decline in quarterly volume we have observed in 2016.

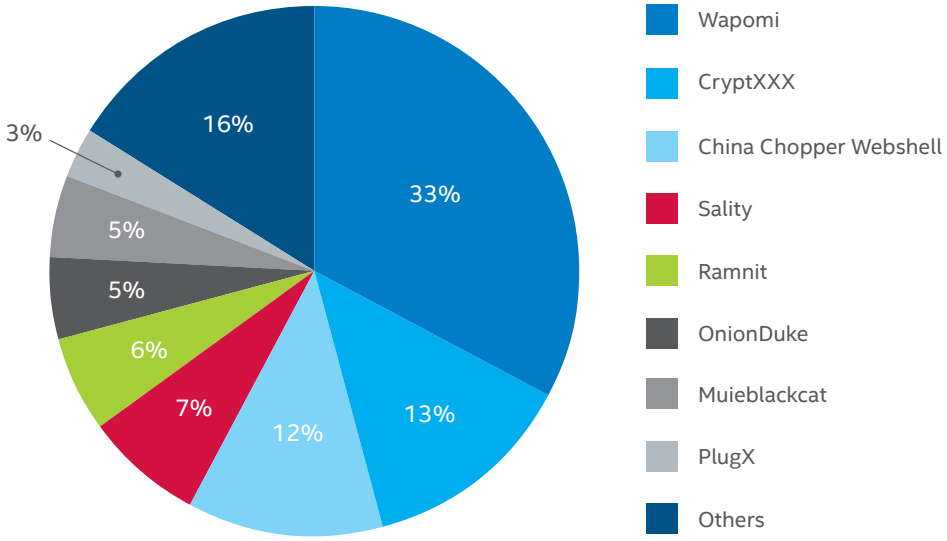
Spam Emails From Top 10 Botnets
(millions of messages)



Source: McAfee Labs, 2016.

Wapomi, which delivers worms and downloaders, remained number one in Q3, declining from 45% in Q2. CryptXXX ransomware served by botnet jumped into second place; it was responsible for only 2% of traffic last quarter.

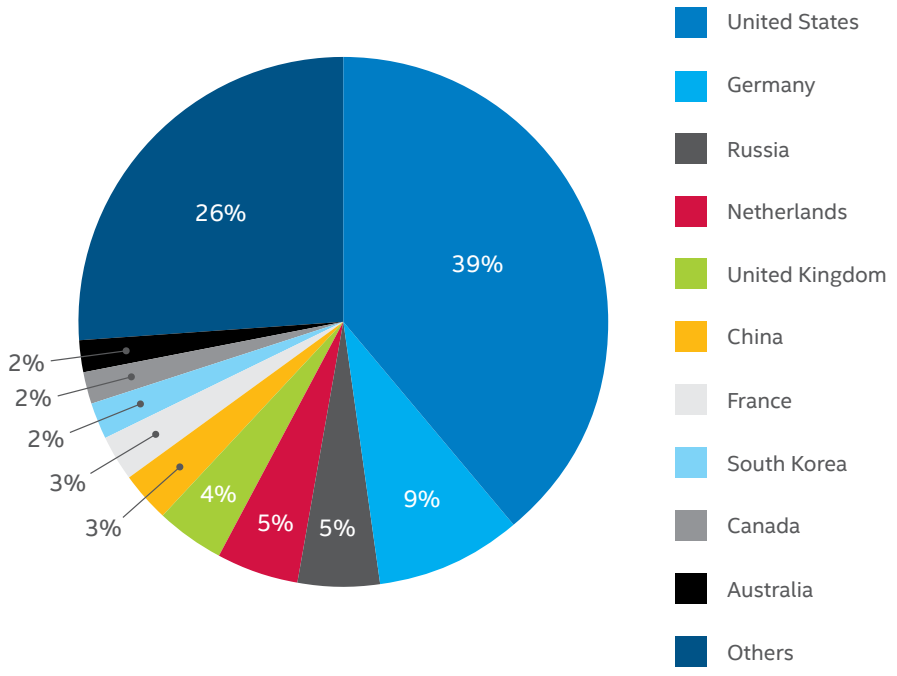
Worldwide Botnet Prevalence



Source: McAfee Labs, 2016.

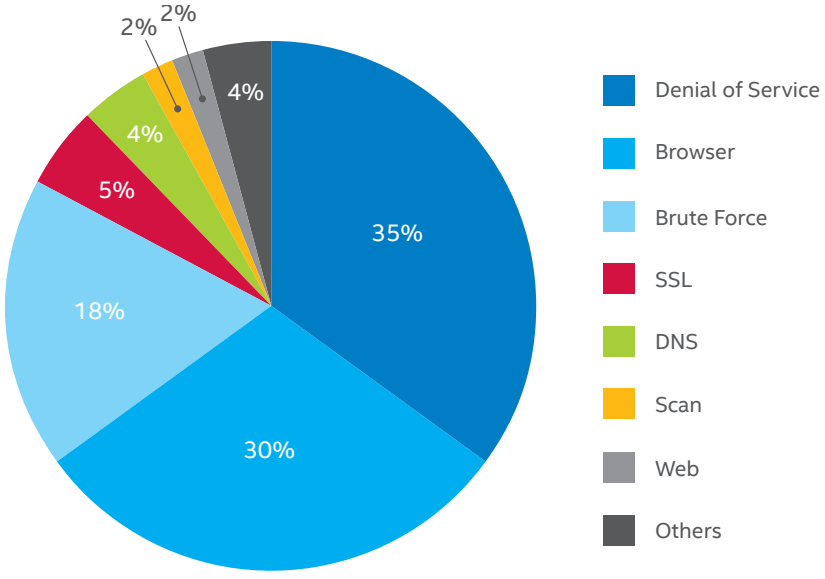
Share this Report

Top Countries Hosting Botnet Control Servers



Source: McAfee Labs, 2016.

Top Network Attacks



Source: McAfee Labs, 2016.

The methods of top network attacks are relatively unchanged from last quarter.

Share this Report

Feedback. To help guide our future work, we're interested in your feedback. If you would like to share your views, please click here to complete a quick, five-minute Threats Report survey.

Follow McAfee Labs

About Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security combines the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world.

www.intelsecurity.com

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

1942_1016_rp-qtrly-threats-report-dec-2016_PAIR
DECEMBER 2016