Report

McAfee Labs
Threats Report

March 2016

Ninety-seven percent of those who share cyber threat intelligence see value in it.

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

The full force of winter is upon us—at least those of us in the Northern Hemisphere—and it is clear that the bad guys have been keeping themselves very busy while stuck indoors.

Our *McAfee Labs 2016 Threats Predictions Report*, published in late November, has been widely read and quoted in the media. Some of the most interesting media coverage comes from The Wall Street Journal, Good Morning America, Silicon Valley Business Journal, and CXO Today. The report includes both near- and long-term views of our cyber security future. If you haven't read it yet, we encourage you to take a look.

And now, as winter's storms have passed, we have published the McAfee Labs Threats Report: March 2016. In this quarterly threats report, we highlight two Key Topics:

- Intel Security interviewed almost 500 security professionals to understand their views and expectations about the sharing of cyber threat intelligence. We learned that awareness is very high and that 97% of those who share cyber threat intelligence see value in it.
- We explore how the Adwind Java-based backdoor Trojan attacks systems through increasingly clever spam campaigns, leading to a rapid increase in the number of Adwind .jar file submissions to McAfee Labs.

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

And in other news…

By the time this report is published, the RSA Conference 2016 will be history. For those who attended, we hope you had a chance to listen to Intel Security's keynote, presented by Chris Young, General Manager of Intel Security Group. Young highlighted two cyber security challenges: the absence of threat intelligence sharing alliances and models, and the talent shortage we face. Given those obstacles, he mapped out a new model for cyber security and shared what is already underway. If you could not attend, a replay is available here. It is well worth a listen.

As we mentioned in the last threats report, McAfee Labs develops much of the core protection technology that becomes part of Intel Security products. In Q4, we released the Real Protect feature in our McAfee Cloud AV—Limited Release product for consumers. It has also been part of our McAfee® Stinger™ malware removal utility for most of 2015. Real Protect is a real-time behavior detection technology that monitors suspicious activity on an endpoint. Real Protect leverages machine learning and automated behavioral-based classification in the cloud to detect zero-day malware in real time. You can learn more about Real Protect here.

Every quarter, we discover new things from the telemetry that flows into McAfee Global Threat Intelligence. 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 Q4, our customers saw the following attack volumes:

- McAfee GTI received on average 47.5 billion queries per day.
- Every day more than 157 million attempts were made (via emails, browser searches, etc.) to entice our customers into connecting to risky URLs.
- Every day more than 353 million infected files were exposed to our customers' networks.
- Every day an additional 71 million potentially unwanted programs attempted installation or launch.
- Every day 55 million attempts were made by our customers to connect to risky IP addresses, or those addresses attempted to connect to customers' networks.

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.

—*Vincent Weafer, Senior Vice President, McAfee Labs*

Contents

McAfee Labs Threats Report
March 2016

This report was researched and written by:

Diwakar Dinkar
Paula Greve
Kent Landfield
François Paget
Eric Peterson
Craig Schmugar
Rakesh Sharma
Rick Simon
Bruce Snell
Dan Sommer
Bing Sun

Executive Summary

The rise of cyber threat intelligence sharing

Intel Security interviewed almost 500 security professionals to understand their views and expectations about cyber threat intelligence sharing. We learned that awareness is very high and that 97% of those who share cyber threat intelligence see value in it.

Security industry expectations are very high that cyber threat intelligence sharing will significantly improve system and network security. But do security practitioners actually see value in sharing cyber threat intelligence? Are they willing to share it themselves and, if so, what are they willing to share? In 2015, Intel Security interviewed almost 500 security professionals in a wide variety of industries and regions, asking these questions and more. Among other things, we learned that awareness is very high and that 97% of those who share cyber threat intelligence see value in it. In this Key Topic, we discuss the promise of cyber threat intelligence sharing and findings from our customer research.

Adwind Java-based malware

The number of Adwind .jar file submissions to McAfee Labs has grown to 7,295 in Q4 2015 from 1,388 in Q1 2015, a 426% increase.

The Adwind remote administration tool (RAT) is a Java-based backdoor Trojan that targets various platforms supporting Java files. Adwind is typically propagated through spam campaigns that employ malware-laden email attachments, compromised web pages, and drive-by downloads. Because spam campaigns are now short lived, with frequently changing subjects and carefully crafted attachments, it has become more difficult for users and security technologies to spot attacks. This has led to a rapid increase in the number of Adwind .jar file submissions from customers to McAfee Labs, with 7,295 in Q4 2015, a leap of 426% from 1,388 in Q1 2015.

Key Topics

Share feedback

The rise of cyber threat intelligence sharing

—Bruce Snell and Kent Landfield

Security professionals must protect against increasingly complex attacks. In the past, they have relied primarily on signature- and behavioral-based defenses to keep threats at bay. Those methods either block a threat by pattern matching or stop it based on suspicious behavior. Both methods are effective and prevent a large percentage of attacks, but what about particularly complex threats, some of which have yet to be discovered? How do we stop zero-day attacks that slip under the radar? That is where cyber threat intelligence comes into play.

When we talk about cyber threat intelligence (CTI), we have to understand that the concept goes much deeper than just a list of IP addresses with poor reputation scores or hashes of suspected bad files. CTI is evidence-based knowledge of an emerging (or existing) threat that can be used to make informed decisions about how to respond. CTI provides more than just the specific bits and bytes of the threat; it also provides context around how the attack takes place. It identifies indicators of attack (IoA) and indicators of compromise (IoC) and potentially even the identity and motivation of the attacker. Security practitioners and security technology can use CTI to better protect against threats or to detect the existence of threats in the trusted environment.

Expectations are high that CTI will significantly improve system and network security when integrated into an organization's infrastructure and operations. Security best practices dictate we push any threat as far as possible from the target. By using CTI, security teams look to not only stop each attack as it happens, but to also get a better sense of who is attacking, what methods they are using, and what their targets are. To do this, we need a bigger picture of what is going on. CTI is key to gaining that level of understanding about the cyber threat.

What is "Cyber Threat Intelligence?"

What activity are we seeing?	Observable	What threats should I look for on my networks and systems, and why?	Indicator
Where has this threat been seen?	Incident	What does it do?	TTP
What weaknesses does this threat exploit?	Exploit Target	Why does it do this?	Campaign
Who is responsible for this threat?	Threat Actor	What can I do about it?	Course of Action

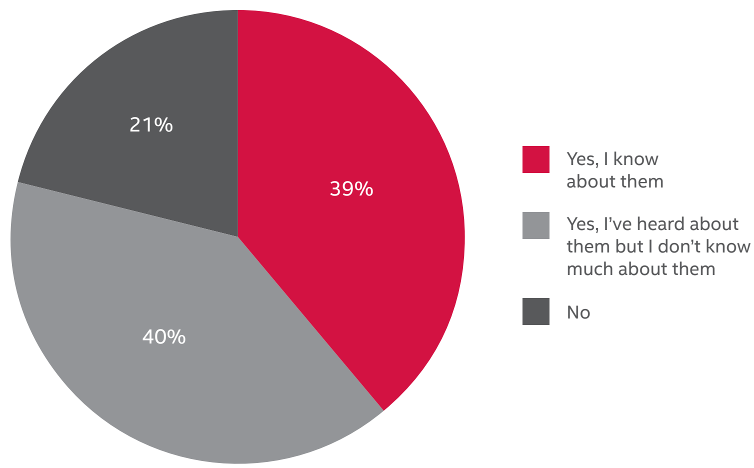
Share this Report

Our research

We often read about CTI and especially the sharing of CTI. But do security experts actually see value in sharing? Are they willing to share it themselves and, if so, what are they willing to share?

In 2015, Intel Security conducted almost 500 interviews with security professionals in a wide variety of industries and regions. Survey respondents included Intel Security customers as well as noncustomers. Here is what we found.

Are You Aware of Any Cyber Threat Intelligence Sharing Initiatives?



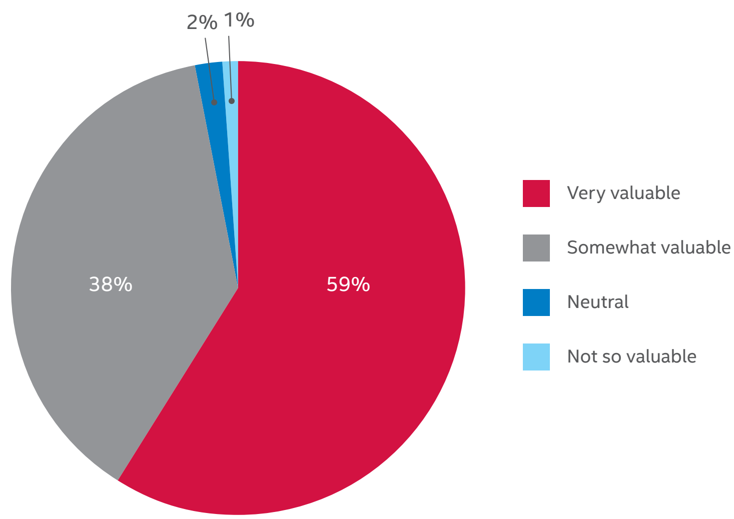
Source: Intel Security survey, 2015.

This is a positive response. When eight out of 10 security professionals are aware of CTI sharing, it means CTI sharing has gained a good bit of mindshare.

We then focused on the group that was aware of CTI sharing and asked if their organizations currently participated in any sort of CTI exchange initiatives. Of these, 42% said they did participate, and 23% were not sure. The remaining 35% said no; they did not participate in any sort of CTI exchange.

Once an organization has started to participate in a CTI exchange, we wanted to see how valuable CTI sharing was to their environment.

How Valuable Is Cyber Threat Intelligence Sharing to Your Organization?

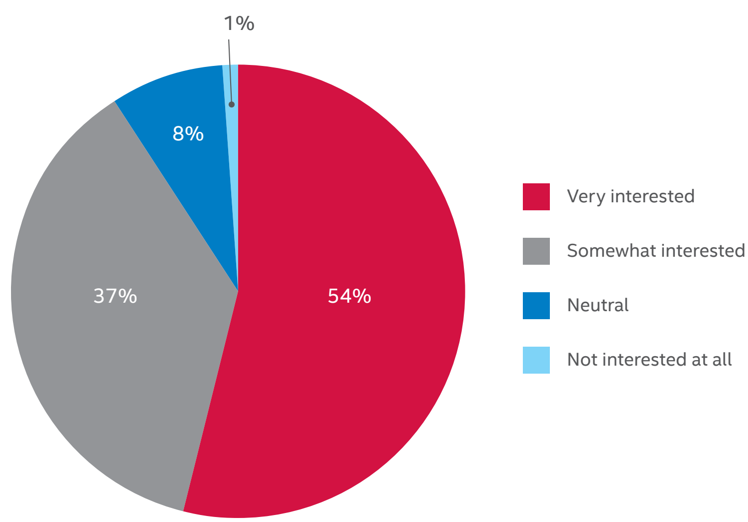


Source: Intel Security survey, 2015.

Once organizations receive CTI through an exchange, a strong majority of them find value in the data.

The majority of shared CTI is industry agnostic. Data is shared across all organizations with no segmentation by industry. We asked whether organizations would be interested in receiving CTI that was directly related to their industry. For example, a CTI exchange between companies in the banking industry or healthcare.

How Interested Would You Be in Receiving Cyber Threat Intelligence Related to Your Industry?



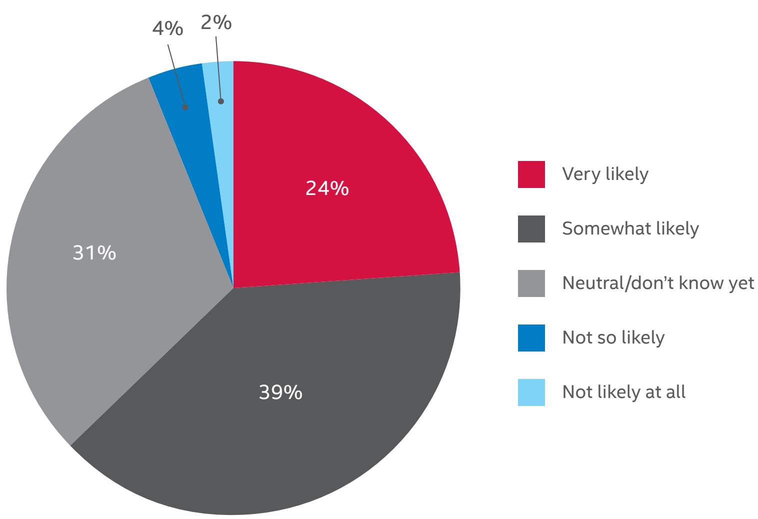
Source: Intel Security survey, 2015.

We found that 91% of respondents interviewed are interested in receiving industry-specific CTI. This makes sense especially in an industry such as banking, in which malware may target multiple financial institutions in similar ways. Critical infrastructure is another area that could benefit from industry-specific information sharing because those organizations might find malware targeted against a specific type of device used only in that industry, as we have seen in the past.

Overall, when asked how they felt about sharing and consuming CTI, 86% agreed that sharing would result in better protection for their company.

Receiving threat data is only part of CTI. For data to be useful to the community, it also has to be *shared*. The survey responses shift a bit when we asked if organizations would be willing to share information with the community. Among those we surveyed, 63% fell into the "very likely" or "somewhat likely" categories.

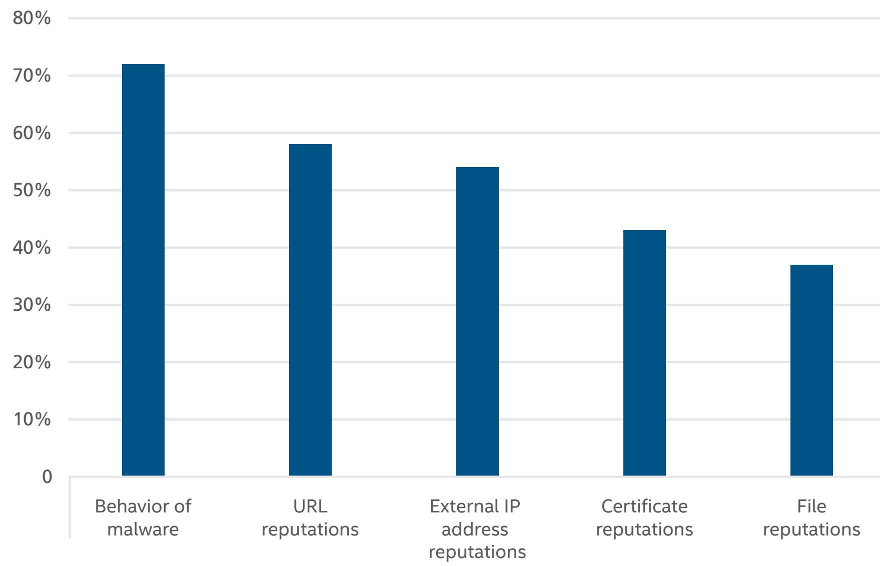
How Likely Would Your Organization Be to Share Cyber Threat Intelligence Reputation Data Within a Secure and Private Platform?



Source: Intel Security survey, 2015.

What sort of data are people willing to share? The most common answer was "behavior of malware," followed by "URL reputations." It is interesting that "file reputation" was the information organizations are least willing to share. We will go into more detail on that in a bit.

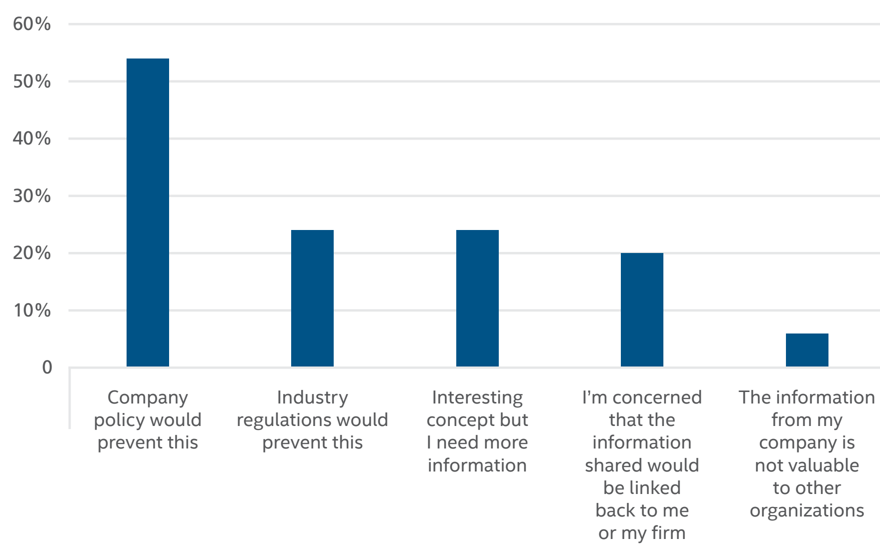
You Indicated a Willingness to Share Some Reputation Data. Which Reputation Data Would You Be Willing to Share?



Source: Intel Security survey, 2015.

We then took the people who responded that they are unwilling to share data and asked why. The leading reason, by a big margin, is corporate policy preventing them from sharing reputation information.

Why Do You Believe Your Organization Would Not Be Willing to Share Reputation Information?



Source: Intel Security survey, 2015.

Share this Report

Why don't companies share cyber threat intelligence?

Policy

With all the benefits of CTI exchanges (Information Sharing and Analysis Centers, CERTs, vendor and industry alliances, trusted partnerships, public/private initiatives, etc.), why are organizations hesitant to share information? Let's look at the type of data least likely to be shared (file reputation) and the high percentage of people responding with "company regulations" as their primary reason for not sharing.

Although Intel Security has discussed CTI sharing with industry participants for a number of years and most agree CTI sharing is likely to be valuable, most balked at sharing file reputation data. We believe the reluctance to share revolves around a misunderstanding of the type of information offered. When sharing file reputation, a hash value is created to represent the file in question. This hash is a unique number used to identify the file, and though it is unique to that file, the hash cannot be used to recreate the file itself. None of the internal file information is sent out of the network and no personally identifiable information (PII) leaves the network. However, when an organization begins to implement a CTI sharing effort, it runs afoul of policies that dictate that no confidential data or PII can leave the organization. This is, of course, generally a good policy but the lack of understanding of the content being shared becomes self-defeating in this case.

Catching bad guys

Another reason some organizations do not want to share reputation data is that it could potentially interfere with an ongoing investigation. Government agencies, military organizations, and industry leaders with sensitive intellectual property have an interest in tracking down who is trying to break into their networks. For these organizations, it often makes sense to allow the exploit to succeed, while monitoring it—in order to gain more information about who is behind the attack and its target, as well as to determine a better way to mitigate future attacks. If the threat data is shared with a CTI community and the attackers participate in that community, they could be alerted that their activities have been identified—resulting in new tactics to avoid further detection. This is one situation in which the evil you know could be better than the evil you do not know.

Concerns over legality

Sharing is as much a legal problem as a technical one. The legal and trust frameworks for sharing cyber threat information are not well established, making it easy for risk-averse corporate lawyers to say no or to set up highly restrictive policies to limit sharing. Much of the sharing today occurs within trusted partnerships with NDAs, MOUs, or other contracts, all of which take some time to be approved by both parties. Often the legal foundation for transient, event-based sharing between two companies does not exist and cannot be established in time to be useful for cyber responders.

Some organizations are hesitant to flag a URL or IP address with a poor reputation due to concerns of potential legal repercussions, such as we have seen when security products have named certain domains as spam generators or labeled a program or add-on as spyware. This concern has expanded to the sharing of CTI.

Concerns over privacy

Privacy is also a major concern. Global laws and norms make sharing an extremely complicated landscape. Regulated organizations must comply with governmental regulations requiring strict controls on items such as customer or patient data. Regulations regarding the sharing of personal information are not always fully understood. To avoid fines and penalties, many err on the side of caution and decide not to share any data with outside organizations except as required to support their business operations.

Exchange standards

For any CTI exchange to work effectively, established technical standards for sharing information are critical. There have been multiple efforts to try to settle on a single format for sharing cyber threat intelligence but most were focused within a specific area, such as incident response. In 2010, MITRE, under the direction of and with funding from the US Department of Homeland Security, began development of a threat information architecture with the goal of producing a representation of an automatable cyber threat indicator. This was the first effort to focus specifically on creating an automatable, structured representation of the cyber-threat lifecycle, related message format, and exchange protocol. The effort produced three specifications:

- TAXII,™ the Trusted Automated eXchange of Indicator Information.
- STIX,™ the Structured Threat Information eXpression.
- CybOX,™ the Cyber Observable eXpression.

Three key standards for sharing cyber threat intelligence.

Source: oasis-open.org.

With the industry's need for these evolving consensus standards to become recognized international standards, the DHS worked with the community to transition the development and ownership of specifications to the Organization for the Advancement of Structured Information Standards (OASIS). OASIS has created the OASIS Cyber Threat Intelligence (CTI) Technical Committee (TC). The CTI TC created subcommittees for each of the specifications, as well as an interoperability subcommittee. OASIS will develop, maintain, and release all future versions of STIX, TAXII, and CybOX.

TAXII is a specification that defines a set of services and message exchanges, which when implemented will enable automated and secure sharing of cyber threat information across organizational as well as product/service boundaries. TAXII allows for the exchange of cyber threat information and is the recommended method for exchanging STIX-formatted CTI.

STIX is the structured format used to convey specific cyber threat information. STIX was developed to address the complete cyber threat lifecycle and provide a consistent machine-readable format. STIX enables automated interpretation via consistent semantics and advanced analysis capabilities. It offers the robust expression of relationships among the individual threat lifecycle components.

STIX uses CybOX, a language for encoding "cyber observables," which may be seen as part of an attack. CybOX provides a standardized representation of "facts" in the cyber domain (both network- and host-based). Cyber observables are elements such as registry keys or key values, file deletions, file hashes, HTTP requests, network subnets, etc. A cyber observable is a measurable event or a stateful property in the cyber domain.

Use of STIX has taken off, with more than 60 vendors using the format to ingest, publish, and exchange cyber threat information. The DHS has standardized US government–related cyber threat data exchange efforts on STIX and TAXII. The security industry is actively building and deploying tools and infrastructure based on these specifications.

Organizational sharing standards and best practices

The security industry is currently undertaking the development of standards and best practices for information sharing and analysis organizations (ISAOs). There are many cyber threat intelligence data feeds, services, and organizations—both commercial and nonprofit—but currently there is no expectation of consistency across them or in what they provide. Most data formats are proprietary and services do not use standard interfaces. Today, sharing organizations are ad hoc in how they deal with their customers and membership. This lack of standards has forced a consuming organization to invest a great deal of time and resources making data useful and actionable—while costing a lot to create and maintain.

Presidential Executive Order 13691 directed the DHS to fund a nongovernmental organization to serve as the ISAO Standards Organization. The ISAO Standards Organization was created to identify a set of voluntary standards and guidelines for the creation, operation, and functioning of cyber sharing and analysis organizations. The intent is to expand the current sector-based model (financial, health, energy, etc.) of Information Sharing and Analysis Centers, enabling the development of innovative types of threat information sharing organizations using standard interoperable interfaces and data formats. The process of cyber threat event data enrichment should influence the types of new cyber threat sharing organizations that will emerge. Although this effort is in the very early stages, it is establishing foundational guidance that will drive the emerging cyber threat intelligence sharing and analysis ecosystem.

The future of cyber threat intelligence

Where are we headed as an industry with CTI sharing? It is one thing to establish policies and standards around sharing, but where do we go after that?

Legal frameworks

A major legal concern is the liability organizations may face if they share CTI with others. In some cases, we have seen antitrust concerns when a set of organizations shares only among themselves. The US Cybersecurity Act of 2015 provides, in part, legal foundations for sharing between government and the private sector and between private sector organizations. The Act directs the DHS and the US Department of Justice to develop guidelines limiting receipt, retention, use, and dissemination of CTI containing personal information by the US federal government. The Act provides liability protection extending to private entities only for systems monitoring and the sharing and receipt of

To learn more about integrating CTI in an Intel Security environment, read the *Operationalizing Threat Intelligence Solution Brief*.

threat indicators in the manner prescribed by the bill. It includes language that there is no requirement to share CTI or defensive measures, or to warn or act based on receipt of CTI or defensive measures. There is also no liability for nonparticipation. The Act also states it is not an antitrust violation for two or more private entities to share threat information for cyber protection purposes.

The clarifications around information sharing with the US government and other entities, as well as the antitrust and the liability protections, allow the security industry to take advantage of cyber threat data in a way not possible before the Act was signed. This Act could become a model for global information sharing legislation. The legal liability relief provided by the Act will help to reduce the fear of sharing and provide the guidelines corporate attorneys have desired.

Increased community sharing

Today we share more threat data than ever, but are we gaining insights into what really matters? Are we finding just opportunistic attacks or are we finding the campaigns that really threaten our operations? In the past, threat feeds, shared information, and security products have not used industry-standard formats. The proprietary nature of data formats has complicated our ability to correlate and use advanced analytics to discover what we should discover. With standard threat data representations, communities of cooperation will be able to review and examine malicious events, attacks, and tools in a much more coordinated fashion than has been possible in the past. This advantage will increasingly occur in for-profit, not-for-profit, and open-source organizations.

Integrated automation

The automated creation, import, and export of CTI is critical for an organization to take advantage of a CTI exchange. Although CTI can be used to manually hunt for threats within an environment, stopping attacks in real time (or near real time) will require automated tools and processes. In order to provide adaptive response and make CTI actionable, security-related products must be able to ingest CTI and act on it without unnecessary human intervention. Formerly, the discovery that a system had malware was limited to that system; today, that information needs to be available throughout the enterprise so an organization can make proper responses. For example, if a malicious file is discovered on an endpoint, notification must be shared across the enterprise's security infrastructure to assure the malware is hunted internally, while blocking attachments at the boundary whose hashes match that of the malicious file. Intelligent responses are possible when security vendors take advantage of standard CTI interfaces and data formats. This standardization allows CTI to be actionable and help reduce the cost of security operations by assuring human resources are not a bottleneck and are used appropriately.

Innovative CTI organizations and services

New security knowledge services are emerging. Much of the past focus of CTI sharing has been on identifying and sharing cyber indicators and observables. A search on "threat intelligence exchange" provides hundreds of results. Although these results contain valid threat indicators, a big problem has been their consistency, type, and quality. When comparing multiple threat exchanges, organizations discover different exchanges provide different content. One may provide a file hash and IP reputation while another contains registry keys and domain name reputation for the same threat. We expect to see CTI aggregators provide standardized feeds in the future.

Although data of this type is vital, we are just beginning to really understand the entire threat lifecycle. As we learn more about a threat, its associated CTI becomes more complete and more valuable. Whole businesses will arise whose only mission is to enrich the data around individual threats to assure their customers have a better picture of what is occurring and how to rapidly mitigate threats to their organizations.

One new organization making CTI actionable is the Cyber Threat Alliance (CTA), which Intel Security helped found. The CTA is a cross-vertical, security vendor initiative whose members share threat information to improve defenses against advanced cyber adversaries who threaten the members' customers. Members share important individual elements of a threat life cycle—including vulnerabilities and exploits, new malware samples, and botnet control infrastructure—that can be incorporated into each member's security products. The CTA's coordinated research allows members to gain insight into the full attack lifecycle of specific campaigns, including in-depth technical analysis and the development of recommendations for prevention and mitigation.

Conclusion

CTI is gaining traction within the security industry as a way to combat advanced threats. As a result of our study, Intel Security found the overall acceptance and desire for CTI is high, but many companies face hurdles to fully realize the benefits of sharing threat data with the community. Some of those hurdles are falling. The use of CTI will become a critical component of organizations' defenses as structured, enriched data will allow organizations to respond more quickly, with a better view of the cyber event landscape.

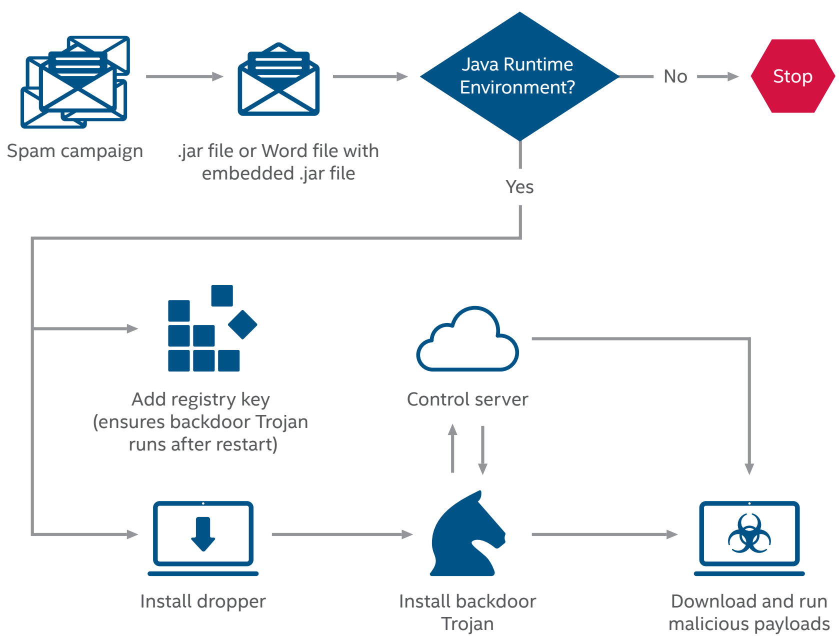
To learn more about integrating CTI in an Intel Security environment, read the *Operationalizing Threat Intelligence Solution Brief*.

Adwind Java-based malware

—Diwakar Dinkar and Rakesh Sharma

The Adwind remote administration tool (RAT) is a Java-based backdoor Trojan that targets various platforms supporting Java files. Adwind does not exploit any vulnerability. Most commonly for an infection to occur, the user must execute the malware by double-clicking on the .jar file that typically arrives as an email attachment, or open an infected Microsoft Word document. Infection begins if the user has the Java Runtime Environment installed. Once the malicious .jar file runs successfully on the target system, the malware silently installs itself and connects to a remote server through a preconfigured port to receive commands from the remote attacker and perform further malicious activities. The number of Adwind .jar file submissions to McAfee Labs has grown to 7,295 in Q4 2015 from 1,388 in Q1 2015, a 426% increase.

Typical Attack Method for Adwind



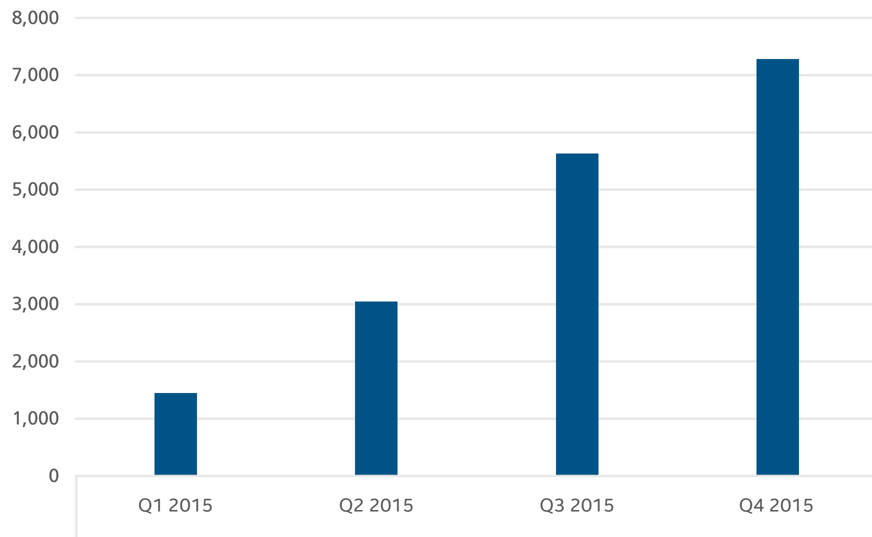
A brief history

Adwind evolved from the Frutas RAT. Frutas is a Java-based RAT, discovered in early 2013, that has been widely used in phishing email campaigns against prominent telecom, mining, government, and finance companies in Europe and Asia. Frutas allows attackers to create a .jar file with backdoor functions that can be executed on a compromised system. Once run, Frutas parses an embedded configuration file to connect to its control server. By the summer of 2013, the name was changed to Adwind. In November 2013, Adwind was rebranded and sold under a new name: UNRECOM (UNiversal REmote COntrol Multiplatform).

Share this Report

Since the beginning of Q3 2015, McAfee Labs has seen a significant rise in.jar file submissions identified as Adwind. The following graph clearly illustrates this:

Adwind .jar File Submissions to McAfee Labs



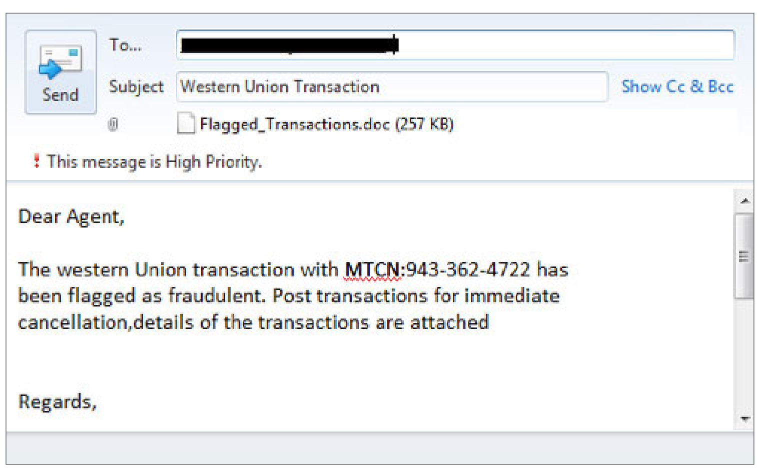
Source: McAfee Labs, 2016.

Infection chain

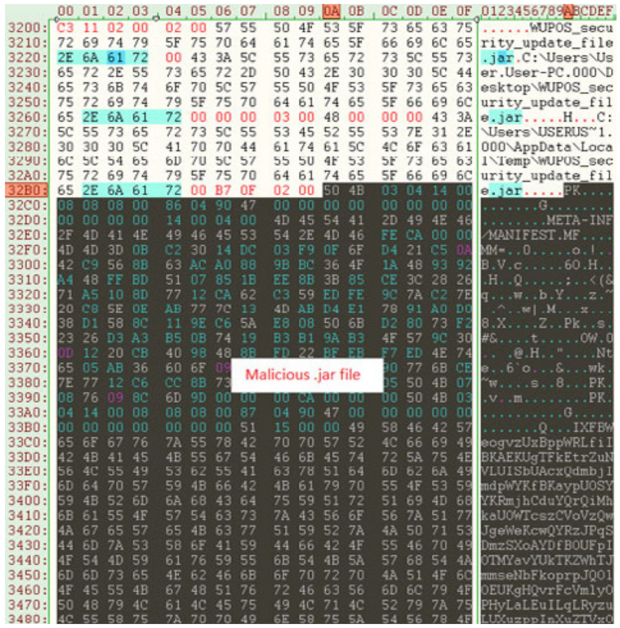
Adwind is typically propagated through spam campaigns that employ malware-laden email attachments, compromised web pages, and drive-by downloads. Its distribution mechanism has evolved: Earlier spam campaigns lasted days and weeks and used the same email subject or attachment name. This consistency helped security vendors quickly detect and mitigate Adwind. Now, spam campaigns are short lived, with frequently changing subjects and carefully crafted attachments, allowing Adwind to avoid detection. Two spam email examples follow:

Example 1: The malicious .jar file is embedded in a Word .doc that upon execution will drop and run the backdoor on the system:

For more information on detecting spoofed emails claiming origin from Western Union, click here.

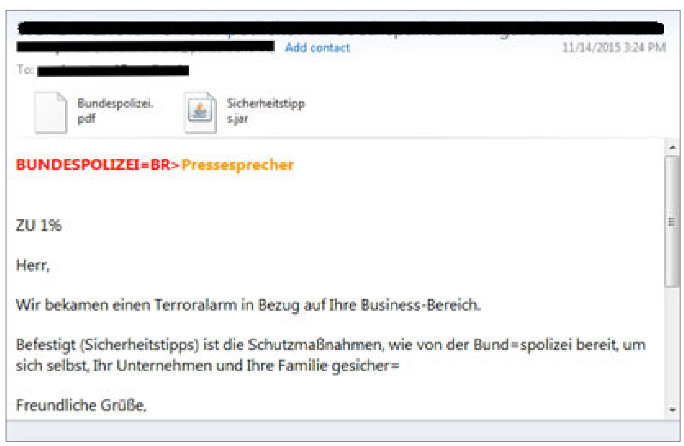


Email message containing infected Word file as an attachment.



Infected Word file contents, including a malicious .jar file.

Example 2: The malicious .jar file also comes as a single attachment or with multiple files attached to an email.



[redacted] Add contact 11/14/2015 3:24 PM

To: [redacted]

Bundespolizei.pdf Sicherheitstipps.jar

BUNDESPOLIZEI=BR>Pressesprecher

ZU 1%

Herr,

Wir bekamen einen Terroralarm in Bezug auf Ihre Business-Bereich.

Befestigt (Sicherheitstipps) ist die Schutzmaßnahmen, wie von der Bund=spolizei bereit, um sich selbst, Ihr Unternehmen und Ihre Familie gesicher=

Freundliche Grüße,

Email message containing a malicious .jar file as an attachment.

The contents of spam email are crafted to lure users using social engineering techniques. Email subject lines include the following:

- ***SPAM*** Re: Payment/TR COPY-Urgent
- Credit note for outstanding payment of Invoice
- Fwd: //Top Urgent// COPY DOCS
- Re:Re: Re:Re:Re TT copy & PIs with Amendments very urgent...
- PO#939423
- Western Union Transaction

The .jar filenames are also crafted to appear benign:

- Shipment_copies (2).jar
- FUD FIle.jar
- PO 8324979(1).jar
- Shipping Documents.jar
- Telex Copy.jar
- INSTRUCTIONCZ121.jar
- Order939423.jar
- Payment TT COPY.jar
- SCAN_DRAFT COPY BL,PL,CI.jar
- Enquiries&Sample Catalog CME-Trade.jar
- Transaction reciept for reconfirmation.xslx.jar
- P-ORD-C-10156-124658.jar
- Proforma Invoice...jar
- TT APPLICATION COPY FORM.jar
- Dec..PO.jar
- Credit_Status_0964093_docx.jar

With an effective subject line and innocently named .jar file, an unsuspecting user could read the email and open the attachment.

Analyzing Adwind variants

Adwind has several variants, which means that the contents of the .jar files can vary.

However, some of the most frequently seen internal file structures are similar in the following variants:

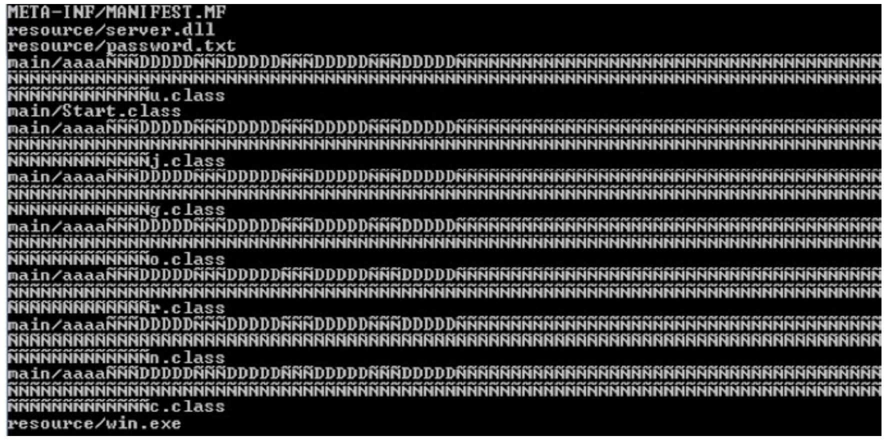
```
META-INF/MANIFEST.MF
config.xml
ID
desinstalador/
extra/
opciones/
Adwind.class
Principal.adwind
desinstalador/MaDe.adwind
desinstalador/desins.class
extra/ClassLoaderMod.class
extra/Constante.class
extra/Constantes$1.class
extra/Constantes$2.class
extra/Constantes$3.class
extra/Constantes.class
opciones/Archivo.class
opciones/Copiar.adwind
opciones/EnviarFile.adwind
opciones/Informacion.adwind
opciones/Instalador.adwind
opciones/Interface_.class
opciones/Opcion1.adwind
opciones/Opcion10.adwind
opciones/Opcion12.adwind
opciones/Opcion15.adwind
opciones/Opcion5.adwind
opciones/Opcion7.adwind
opciones/Opcion7b.adwind
opciones/Opcion8.adwind
opciones/Opcion9.adwind
opciones/Opcion9b.adwind
opciones/OrdenCaptura.class
opciones/Pina.adwind
opciones/RecibirFile.adwind
opciones/WebBot.adwind
opciones/a.png
opciones/interfaceInfo.class
extra/Constante$Constante.class
extra/Constante$ClassLoaderMod.class
extra/Constantes$Constantes$2.class
Adwind$2.class
extra/Constantes$ClassLoaderMod.class
opciones/Interface_$Archivo.class
opciones/Interface_$interfaceInfo.class
Adwind$1.class
extra/Constantes$Constantes.class
Adwind$0.class
extra/Constante$Constantes$2.class
desinstalador/desins$2.class
desinstalador/desins$0.class
extra/Constante$Constantes$3.class
desinstalador/desins$1.class
extra/ClassLoaderMod$Constantes.class
```

Adwind variant 1, showing manifest.mf.

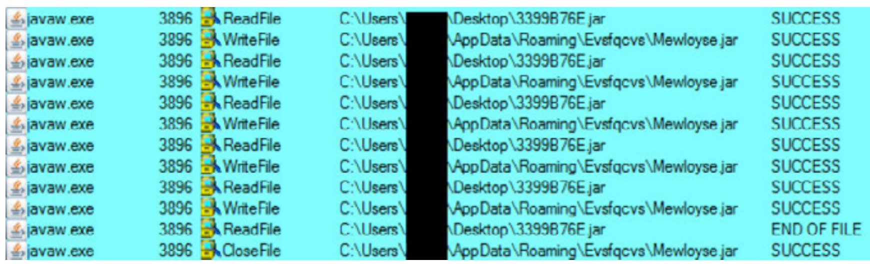
```
META-INF/MANIFEST.MF
h9umf51nbTqbNr7jtUfQ//ETYEKSRsJMGsSPYn4rvcVoSEbY/Xg484Nyr0BBYRvpUYzWCEb/ACuhP2tX
/koodZIhDl/PM30w//B2yZvPw605CrqHMNIQZumya/w8Kyq/kXOpQZ4DdBe0p/7r2tNn5Y5KTT1NnhXN
1Hh5weX/GmUiSDDor01ryrCAQ7Jvk/3jmN/Th3GRXKvFZqjBXxbaNuSkhtY8YE/0KM/5rReTIGEUV0h3
niGKOeESJep/FCMxDY2B4f3y2IiBHtQ4BX0OKI/DDGHsnTzf9cya61MV1j68VAM/QL1sv1aEo
config/config.perl
main/AuX.class
main/CON.class
main/Start.class
main/coN.class
main/nul.class
main/prn.class
main/Aux.class
main/AUx.class
main/nUl.class
main/cON.class
main/aUx.class
```

Adwind variant 2, showing manifest.mf.

Share this Report

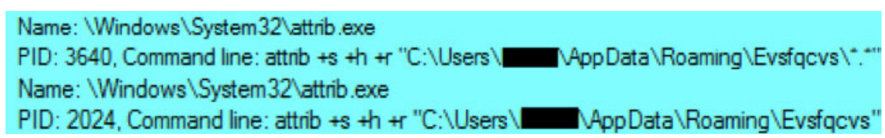


Adwind variant 3, showing manifest.mf.

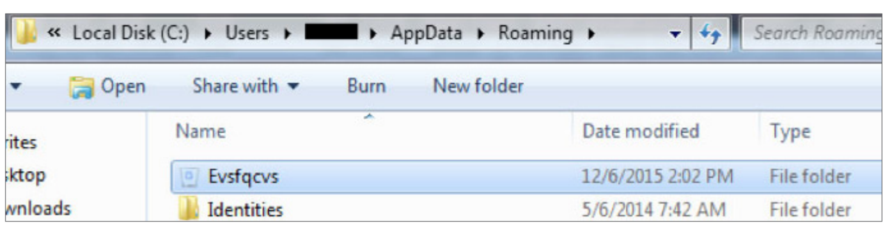


On execution, Adwind copies itself to %AppData%\[random folder name]\[random filename].jar.

Depending on the variant of Adwind, the Java archive copied in the %AppData% folder may use a different file extension than .jar: %AppData%\[random folder name]\[random filename].[random file extension].



The Trojan changes the folder and file attributes to system, hidden, and read only.



The random folder created by Adwind.

Finally, Adwind executes the copy of itself located in the %AppData% folder and adds the following registry key, which will enable the Java backdoor Trojan to run at start-up:

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\
Run] "[random value name"="[Java Runtime Environment directory]\
javaw.exe" – jar "%AppData%\[random folder name]\[random filename].
jar"
```

An Adwind registry key.

Name	Type	Data
(Default)	REG_SZ	(value not set)
Psyajrgr	REG_SZ	"C:\Program Files\Java\jre1.8.0_66\bin\javaw.exe" -jar "C:\Users\[redacted]\AppData\Roaming\Evsfqcvs\Mewloyse.jar"

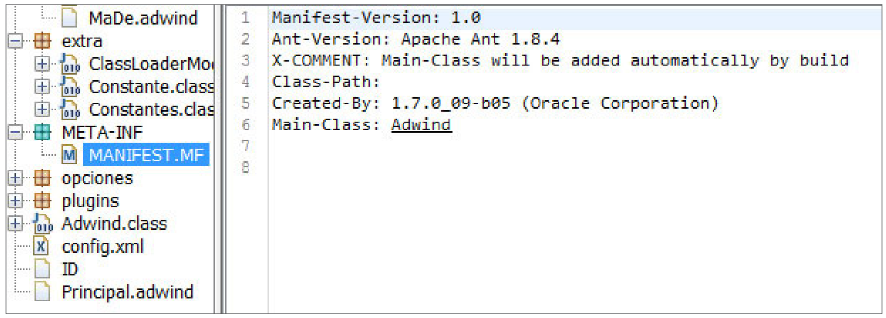
The Adwind registry key with random names assigned.

Adwind comes in an obfuscated form to hide its malicious intent. Its payload and configuration file (which serves as an installation file) are encrypted with the DES, RC4, or RC6 cipher, depending on the variant. The Adwind backdoor will decrypt itself on the fly during execution.

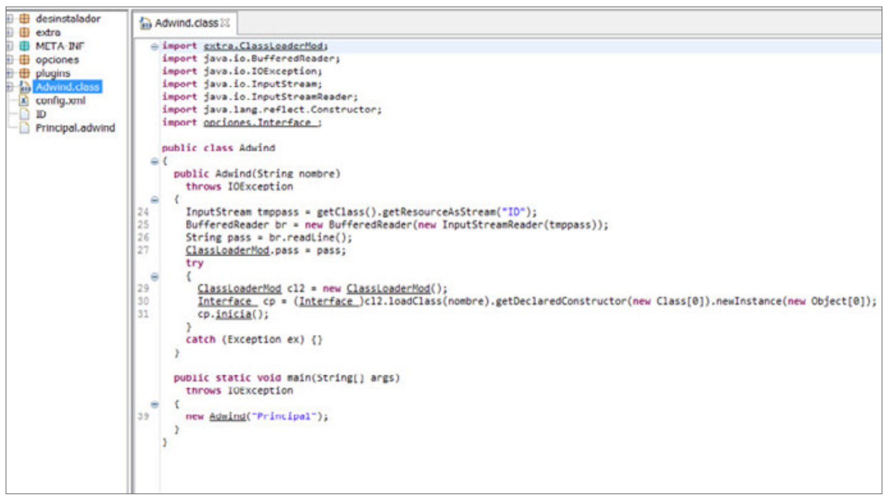
- Variant 1

```
META-INF/MANIFEST.MF
config.xml
ID
desinstalador/
extra/
opciones/
Adwind.class
Principal.adwind
desinstalador/MaDe.adwind
desinstalador/desins.class
extra/ClassLoaderMod.class
extra/Constante.class
extra/Constantes$1.class
extra/Constantes$2.class
extra/Constantes$3.class
extra/Constantes.class
opciones/Archivo.class
opciones/Copiar.adwind
opciones/EnviarFile.adwind
opciones/Informacion.adwind
opciones/Instalador.adwind
opciones/Interface_.class
opciones/Opcion1.adwind
opciones/Opcion10.adwind
opciones/Opcion12.adwind
opciones/Opcion15.adwind
opciones/Opcion5.adwind
opciones/Opcion7.adwind
opciones/Opcion7b.adwind
opciones/Opcion8.adwind
opciones/Opcion9.adwind
opciones/Opcion9b.adwind
opciones/OrdenCaptura.class
opciones/Pina.adwind
opciones/RecibirFile.adwind
opciones/WebBot.adwind
opciones/a.png
opciones/interfaceInfo.class
extra/Constante$Constante.class
extra/Constante$ClassLoaderMod.class
extra/Constantes$Constantes$2.class
Adwind$2.class
extra/Constantes$ClassLoaderMod.class
opciones/Interface_$Archivo.class
opciones/Interface_$interfaceInfo.class
Adwind$1.class
extra/Constantes$Constantes.class
Adwind$0.class
extra/Constante$Constantes$2.class
desinstalador/desins$2.class
desinstalador/desins$0.class
extra/Constante$Constantes$3.class
desinstalador/desins$1.class
extra/ClassLoaderMod$Constantes.class
```

The first class to be executed is Adwind.class, as shown in the meta-inf/manifest.mf file.

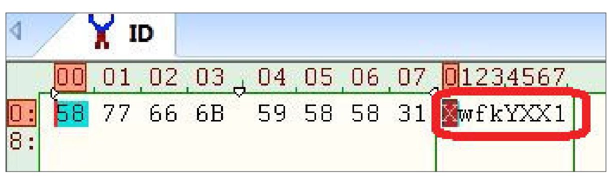


Variant 1's manifest.mf.



Variant 1's Adwind.class.

The file ID is read in and its first line is stored as a string in the variable "pass." Then, ClassLoaderMod is loaded with the variable "pass" and the string "Principal."

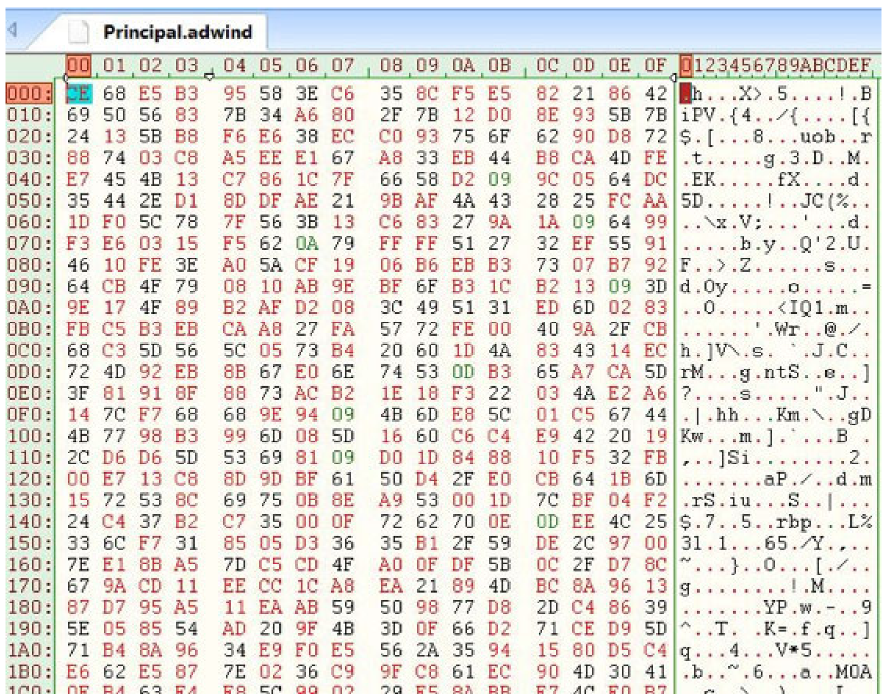


The content of the variable "pass" retrieved from the ID file is an eight-character string.

```java
package extra;

import java.io.ByteArrayInputStream;
import java.io.ByteArrayOutputStream;
import java.io.IOException;
import java.io.InputStream;
import java.util.zip.GZIPInputStream;

public class ClassLoaderMod
  extends ClassLoader
{
  public static String pass;

  public Class findClass(String name)
  {
    byte[] b = loadClassData(name);
    return defineClass(name, b, 0, b.length);
  }

  private byte[] loadClassData(String name)
  {
    byte[] tmp = null;
    InputStream m = getResourceAsStream(name.replace(".", "/").concat(new String(new char[] { '.', 'a', 'd', 'w', 'i', 'n', 'd' })));
    ByteArrayOutputStream b = new ByteArrayOutputStream();
    try
    {
      byte[] buf = new byte['Ȁ'];
      int i;
      while ((i = m.read(buf)) > -1) {
        b.write(buf, 0, i);
      }
      b.close();
```

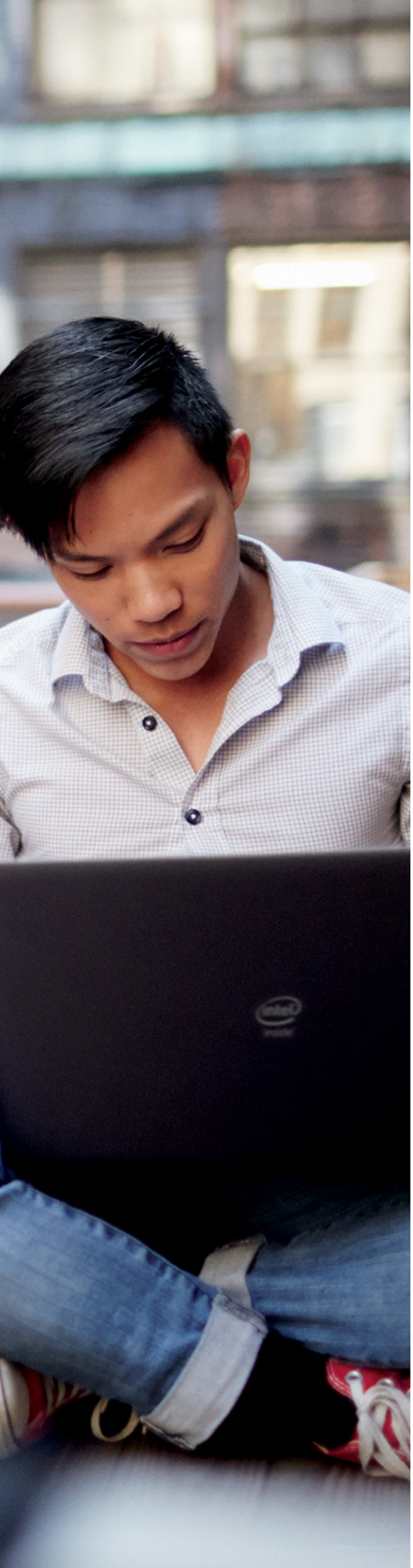
The ClassLoaderMod.

The ClassLoaderMod class adds the string “Principal” to the series of characters to create a new string Principal.adwind, which is another resource file located in the Java archive. However, this file appears to be encrypted:



The encrypted file Principal.adwind.

Share this Report



Then, the eight-character string previously retrieved from the file ID and Principal.adwind are passed to the method Constantino, located in the file Constante.class. This method is in charge of the decompression (using a GZIP method) of the Principal.adwind resource file and its decryption using the DES cipher:

```
Constante.class

package extra;

import java.io.ByteArrayOutputStream;
import javax.crypto.Cipher;
import javax.crypto.SecretKey;
import javax.crypto.SecretKeyFactory;
import javax.crypto.spec.DESKeySpec;

public class Constante
{
  public static byte[] Constantino(String contrasena, byte[] input)
  {
    try
    {
      ByteArrayOutputStream out = new ByteArrayOutputStream();
      SecretKeyFactory skf = SecretKeyFactory.getInstance(new String(new char[] { 'D', 'E', 'S' }));
      DESKeySpec kspec = new DESKeySpec(contrasena.getBytes());
      SecretKey ks = skf.generateSecret(kspec);
      Cipher c = Cipher.getInstance(new String(new char[] { 'D', 'E', 'S' }));
      c.init(2, ks);
      byte[] tmp = c.update(input, 0, input.length);
      out.write(tmp);
      tmp = c.doFinal();
      out.write(tmp);
      out.close();
      return out.toByteArray();
    }
    catch (Exception ex) {}
    return null;
  }
}
```

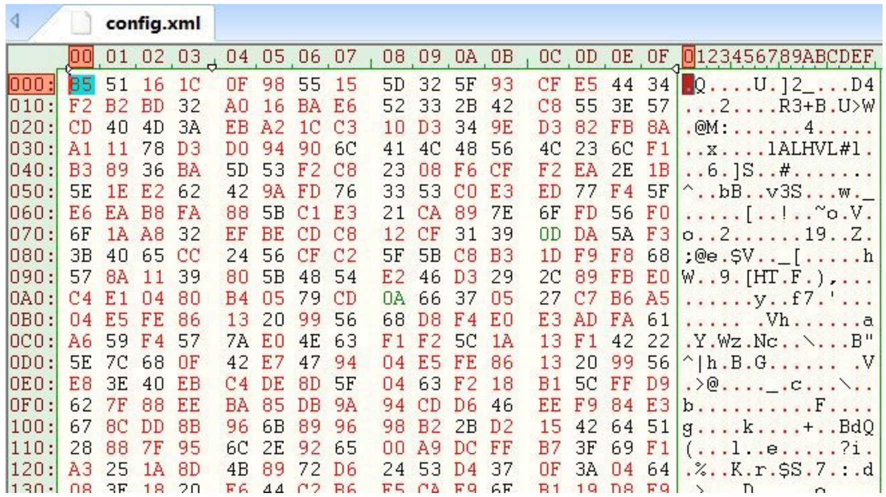
The constante.class method decompresses and decrypts Principal.adwind.

Once decrypted, Principal.adwind appears to be another class file. This class file may look like:

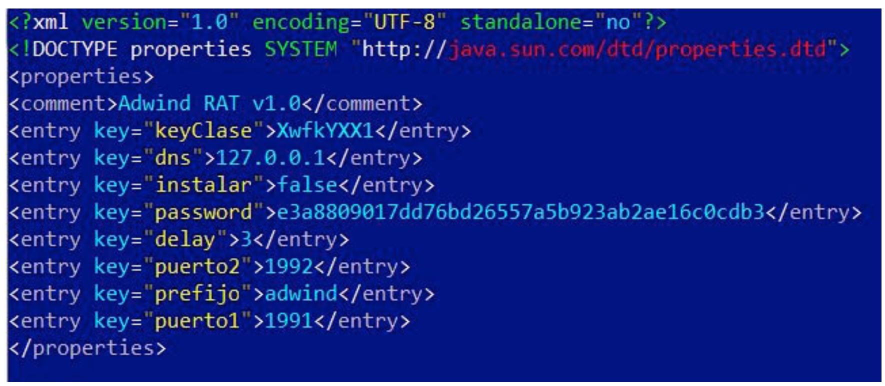
```
import extra.*;
import java.io.*;
import java.lang.reflect.Constructor;
import java.util.Properties;
import javax.swing.UIManager;
import opciones.Interface_;
import plugins.PluginsTotales_in;
public class principal implements Interface_ {
 public void loadMANIFEST() {
  try {
   try {
    uimanager.setLookAndFeel(uimanager.getSystemLookAndFeelClassName());
    uimanager.put("AuditoryCues.playList", uimanager.get("AuditoryCues.allAuditoryCues"));
   } catch (exception e) {}
   properties p = new properties();
   inputstream in = getClass().getResourceAsStream("config.xml");
   byte buf[] = new byte[1024];
   bytearrayoutputstream out = new bytearrayoutputstream();
   int i;
   while ((i = in .read(buf)) > -1) out.write(buf, 0, i);
   out.close();
   byte desenc[] = Constante.Constantino("awenubisskqi", out.toByteArray());
   bytearrayinputstream input = new bytearrayinputstream(desenc);
   p.loadFromXML(input);
   Constantes.attrs = p;
  } catch (ioexception ex) {}
 }
 public principal() throws ioexception {
  try {
   uimanager.setLookAndFeel(uimanager.getSystemLookAndFeelClassName());
   uimanager.put("AuditoryCues.playList", uimanager.get("AuditoryCues.allAuditoryCues"));
  } catch (exception e) {}
```

Principal.adwind posing as a class file.

This file contains the hardcoded key "awenubisskqi," which decrypts the file config.xml (DES decryption again), and acts as the backdoor installer by reading the decrypted config.xml.



Config.xml in its encrypted form.



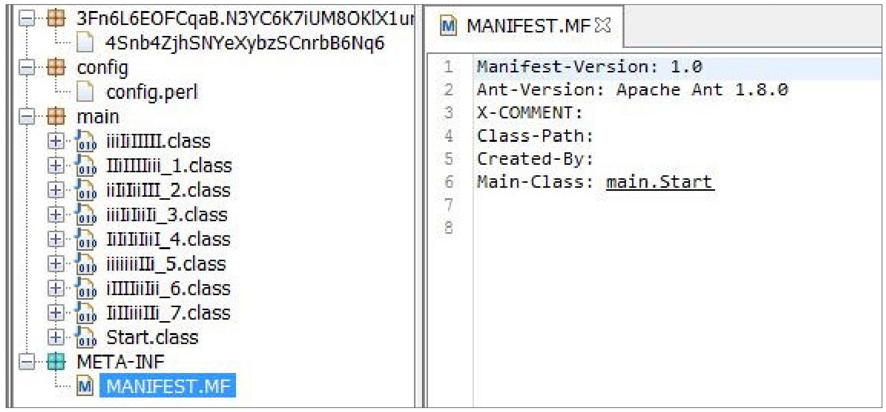
```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>Adwind RAT v1.0</comment>
<entry key="keyClase">XwfkYXX1</entry>
<entry key="dns">127.0.0.1</entry>
<entry key="instalar">false</entry>
<entry key="password">e3a8809017dd76bd26557a5b923ab2ae16c0cdb3</entry>
<entry key="delay">3</entry>
<entry key="puerto2">1992</entry>
<entry key="prefijo">adwind</entry>
<entry key="puerto1">1991</entry>
</properties>
```


The contents of config.xml after decryption.

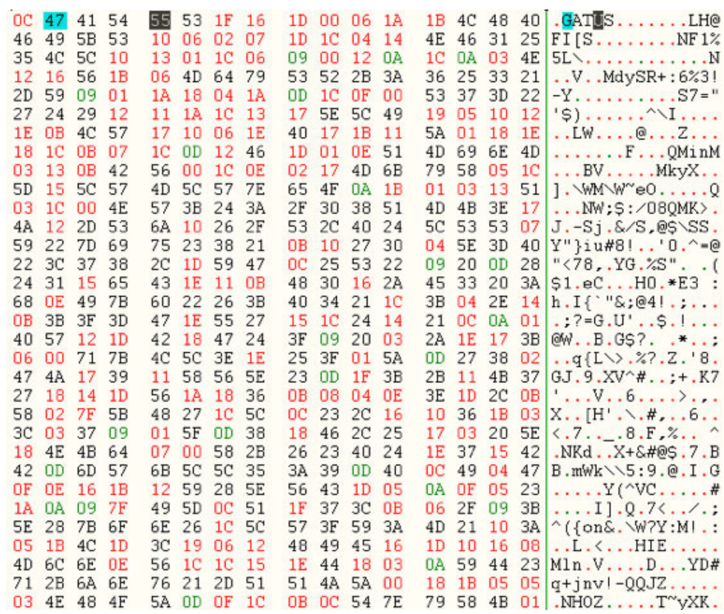
The contents of config.xml vary from one sample to another and are parsed and used to configure and launch further malicious activities. All the other files ending with .adwind in the Java archive will be decrypted on the fly in the same way. Also, depending on the plug-ins used (additional class files), the backdoor will have more or fewer functions. Some plug-ins can allow the attacker to take screenshots of the victim's system, download and execute additional files, modify and delete some files, record keystrokes, access the webcam, control the mouse and keyboard, update itself, etc.

Other variants are decrypted differently:

- Variant 2



In variant 2 the main entry specified in manifest.mf is start.class.



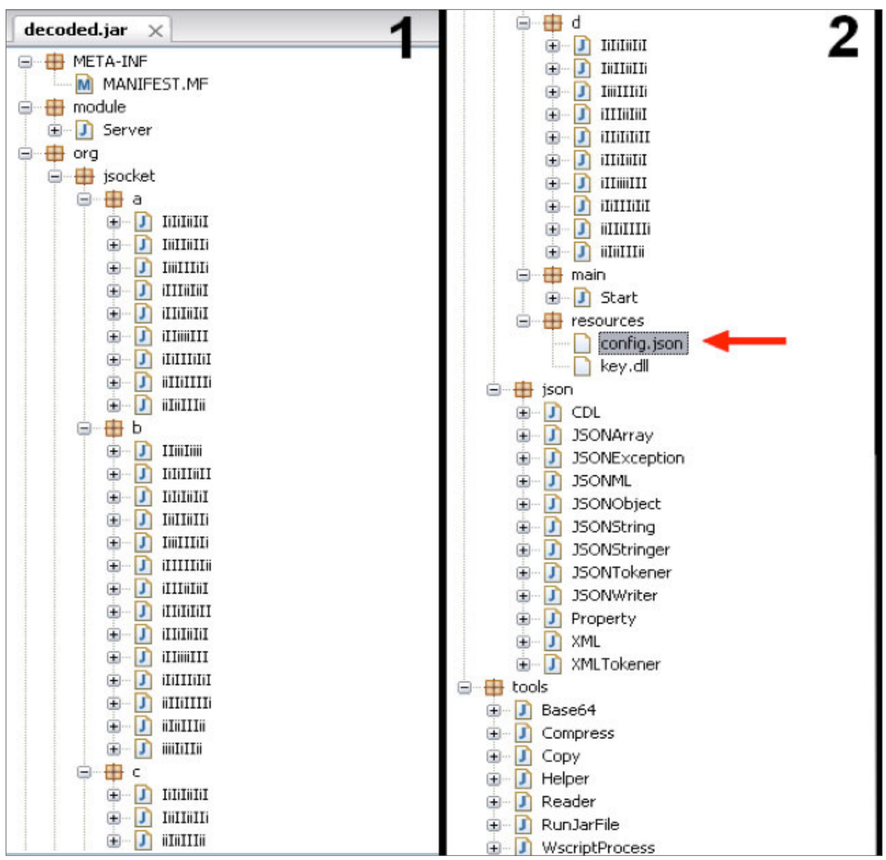
Config.perl is an XOR-encrypted text file.

```
db '<?xml version="1.0" encoding="UTF-8" standalone="no"?>',0Dh,0Ah
db '<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.d'
db 'td">',0Dh,0Ah
db '<properties>',0Dh,0Ah
db '<comment/>',0Dh,0Ah
db '<entry key="SERVER">/h9umf51nbTqbNr7jtUfQ//ETYEKSRsJMGsSPYn4rvcVo'
db 'SEbY/Xg484NyrUBBYRvpUYzWCEb/ACuhP2tX/kood2IhDl/PM30w//B2yZvPw605C'
db 'rqHMNIQZumya/w8Kyq/kX0pQZ4DdBe0p/7r2tNn5Y5KTT1NnhXNlHh5weX/GmUiSD'
db 'Dor01ryrCAQ7Jvk/3jmN/Th3GRXKvFZqjBXxbaNuSkhtY8YE/0KM/5rReTIGEUV0h'
db '3niGKOeESJep/FCMxDY2B4f3y2IiBHtQ4BX0OKI/DDGHsnTzf9cya61MVlj68VAM/'
db 'QL1sv1aEo</entry>',0Dh,0Ah
db '<entry key="PASSWORD">q3VnExXMR4</entry>',0Dh,0Ah
db '</properties>',0Dh,0Ah
```

Decrypted content from config.perl.

We can see this code contains the randomly chosen path and filename for the embedded and encrypted malicious .jar file, and half of the RC6 key that will be used to decrypt it. The other half of the RC6 key is retrieved from the other available class files. In the preceding code QL1sv1aEo is the RC6-encrypted malicious .jar file containing the Adwind backdoor.

After decrypting the encrypted .jar file, we can gain access to the Adwind backdoor class files and resources.

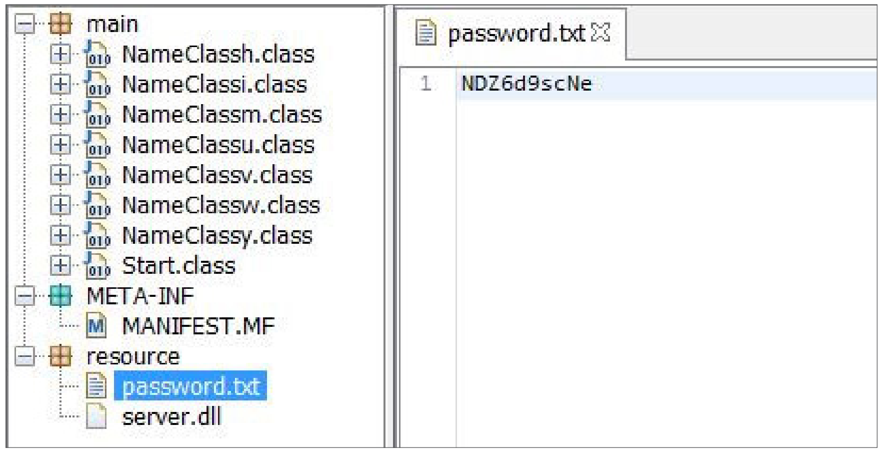


The file config.json is the configuration file (in plain text) of the backdoor, containing the defined port numbers, servers, the installation path, etc.

Share this Report

- Variant 3

The main entry specified in manifest.mf is start.class. Password.txt, in plain text, contains half of the RC6 key used to decrypt the embedded malicious .jar file. The other half of the RC6 key is retrieved from the other available class files. Server.dll is the RC6-encrypted malicious .jar file containing the Adwind backdoor.



Adwind variant 3's password.txt appears in plain text.

Restart mechanism

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] "[random value name"="[Java Runtime Environment directory]\jawaw.exe" – jar "%AppData%\[random folder name]\[random filename].jar"

This registry entry confirms that the backdoor Trojan will start every time Windows starts.

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] "[random value name"="[Java Runtime Environment directory]\jawaw.exe" – jar "%AppData%\[random folder name]\[random filename].[random extension name]"

This registry entry is for newer variants using a random Java archive file extension.

Post-infection attacks

After Adwind successfully infects a system, we have seen it log keystrokes, modify and delete files, download and execute further malware, take screenshots, access the system's camera, take control of the mouse and keyboard, update itself, and more.

To learn how Intel Security products can help protect against Adwind and other malicious remote administration tools, read the *Stopping Backdoor Trojans Solution Brief*.

Detection and prevention

The following indicators of compromise can be used to identify Adwind-infected systems in an automated way:

```
"%AppData%\[random folder name]\[random filename].jar"
```

Files dropped in the administrator application data folder.

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run] "[random
value name"="[Java Runtime Environment directory]\javaw.exe" – jar
"%AppData%\[random folder name]\[random filename].jar"
```

Run key in the registry.

McAfee Labs recommends the following steps to combat .jar malware such as Adwind:

- Keep systems current by applying the latest security technology updates and antimalware definitions.
- Enable automatic operating system updates, or download operating system updates regularly, to keep them patched against known vulnerabilities.
- Configure antimalware software to automatically scan all email and instant-message attachments.
- Make sure email programs do not automatically open attachments or automatically render graphics, and turn off the preview pane.
- Configure browser security settings to medium level or above.
- Use great caution when opening attachments, especially when those attachments carry the .jar, .pdf, .doc, or .xls extension.
- Never open unsolicited emails or unexpected attachments—even from known people.
- Beware of spam-based phishing schemes. Don't click on links in emails or instant messages.

To learn how Intel Security products can help protect against Adwind and other malicious remote administration tools, read the *Stopping Backdoor Trojans Solution Brief*.

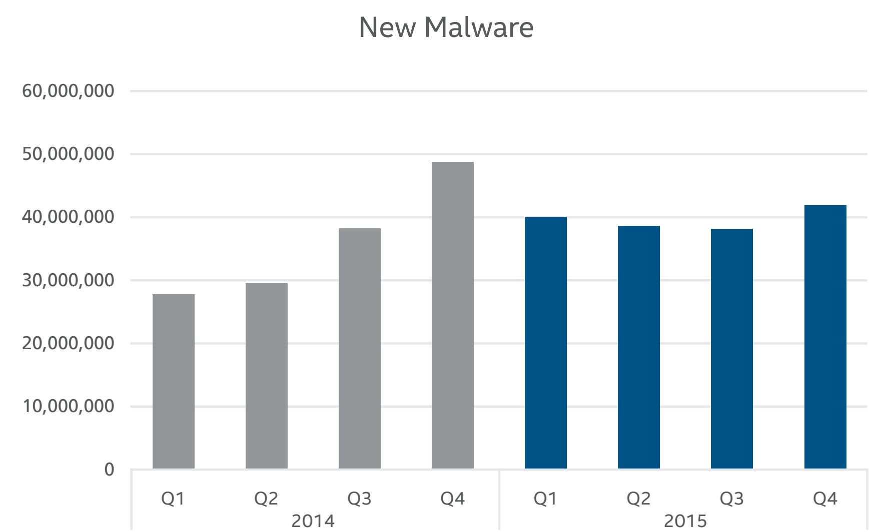
Threats Statistics

Share feedback

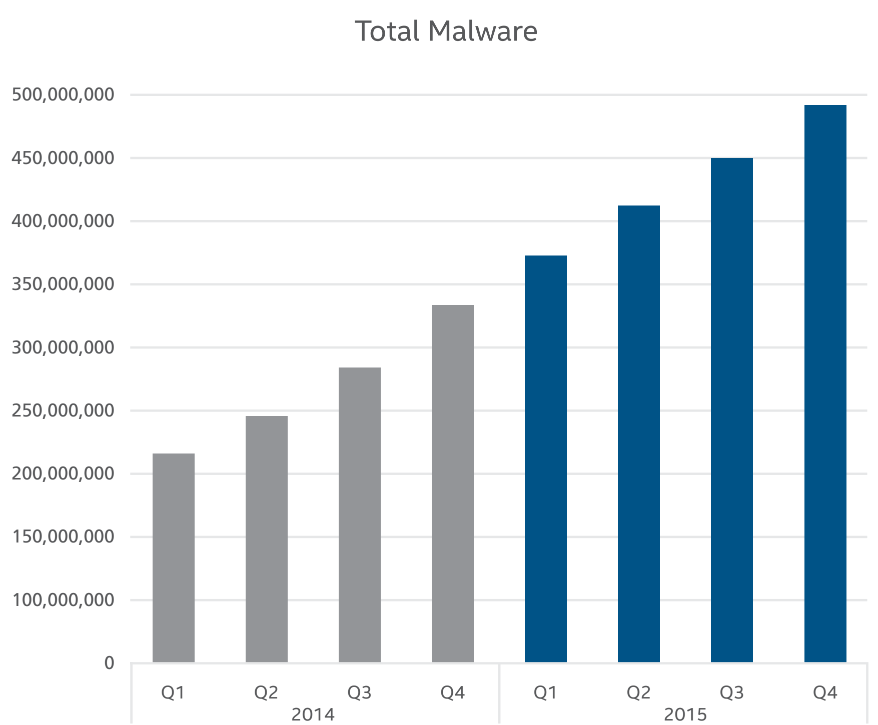
Malware

In this threats report, we adjusted our malware sample counting method to increase its accuracy. This adjustment has been applied to all quarters shown in the new malware and total malware charts.

After three quarters of decline, the number of new malware samples resumed its ascent in Q4, with 42 million new malicious hashes discovered, 10% more than in Q3 and the second highest on record. The growth in Q4 was driven, in part, by 2.3 million new mobile threats, 1 million more than in Q3.



Source: McAfee Labs, 2016.

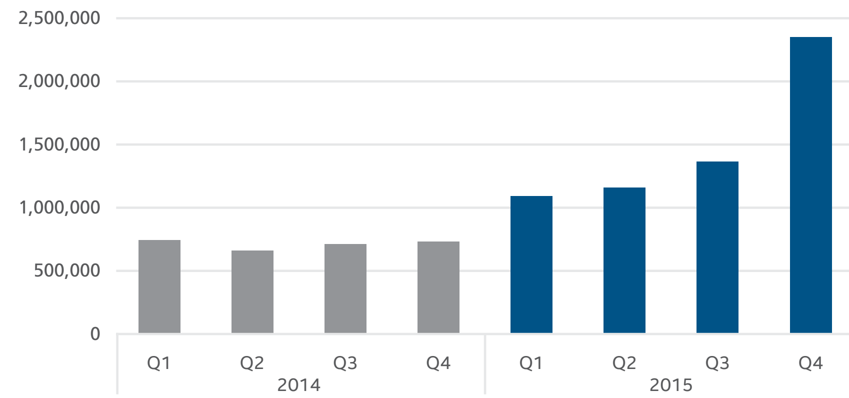


Source: McAfee Labs, 2016.

Share this Report

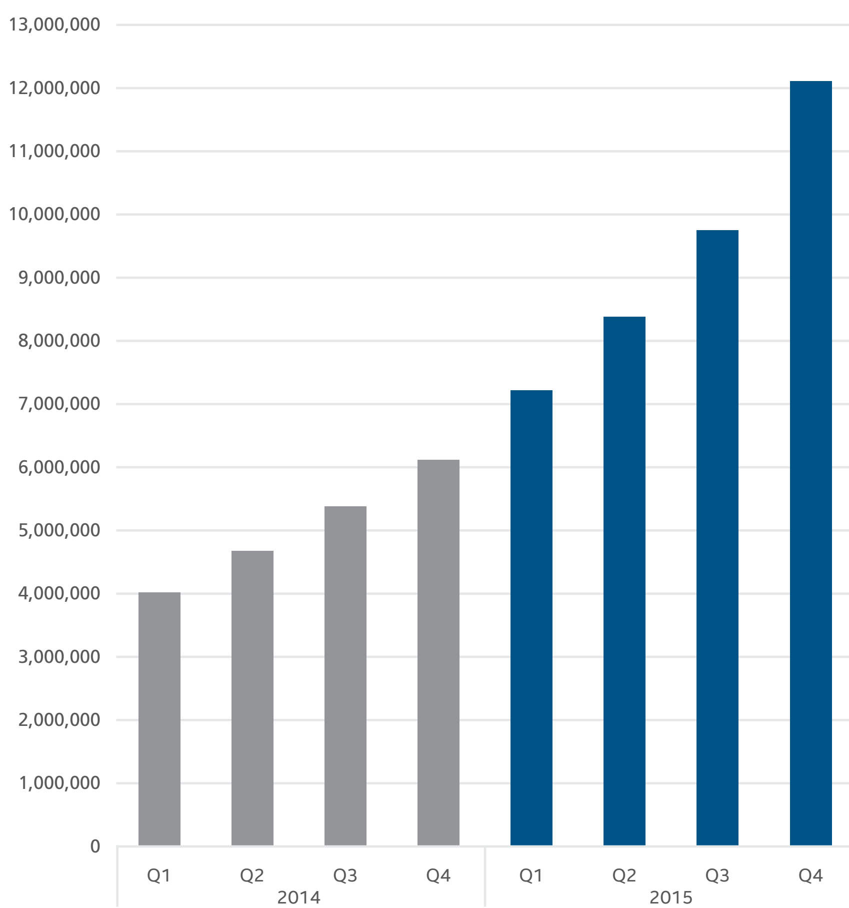
This quarter we recorded a 72% increase in new mobile malware samples. We believe that Google's August 2015 notification that it would release monthly updates to its Android mobile operating system forced malware authors to develop new malware more frequently in response to the enhanced security in each monthly release of the operating system. The detection of newly developed mobile malware is reflected in our Q4 statistics.

New Mobile Malware



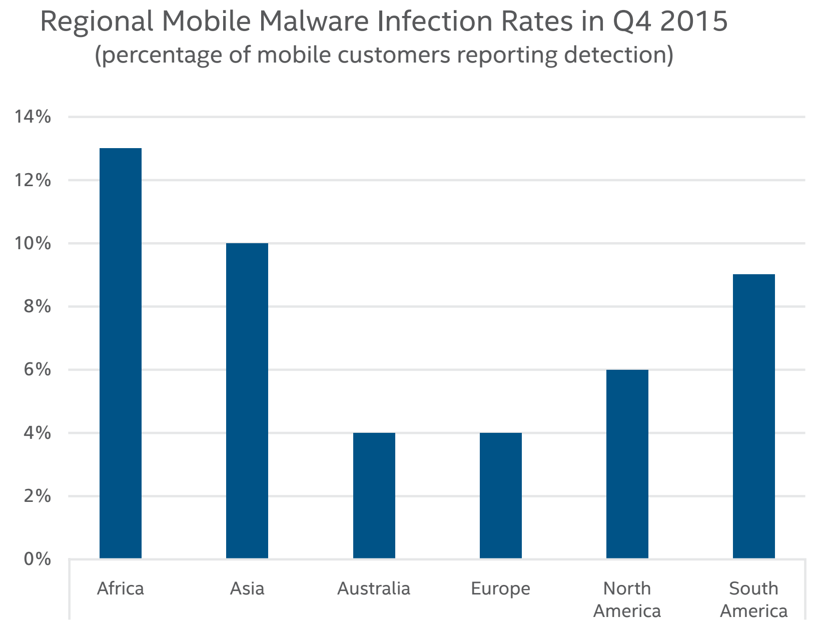
Source: McAfee Labs, 2016.

Total Mobile Malware

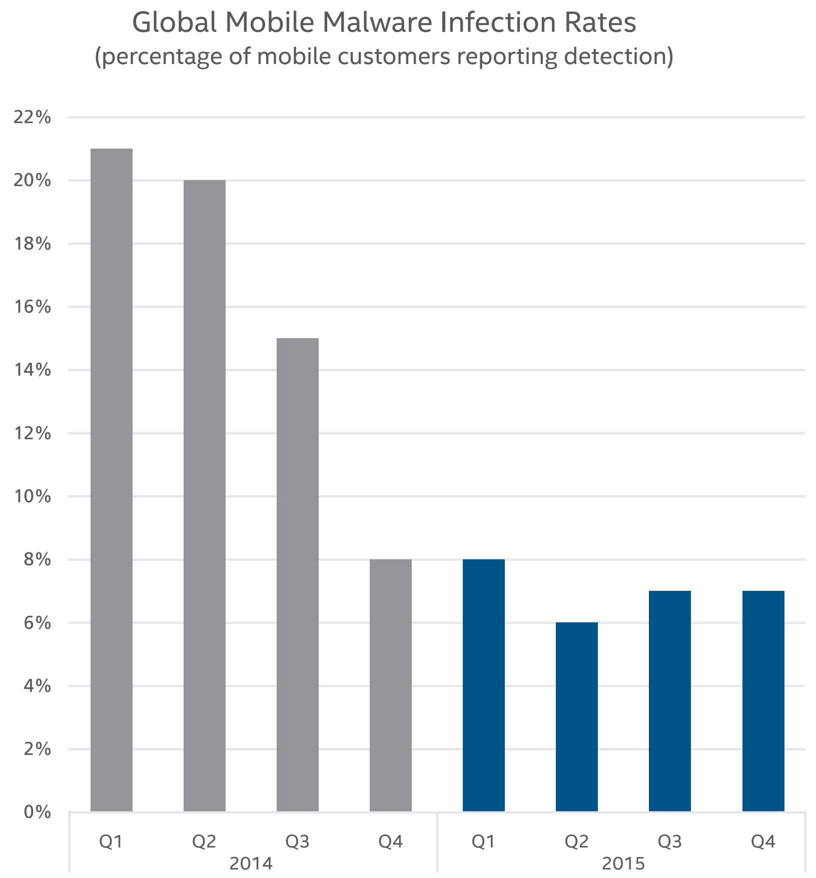


Source: McAfee Labs, 2016.

Share this Report



Source: McAfee Labs, 2016.

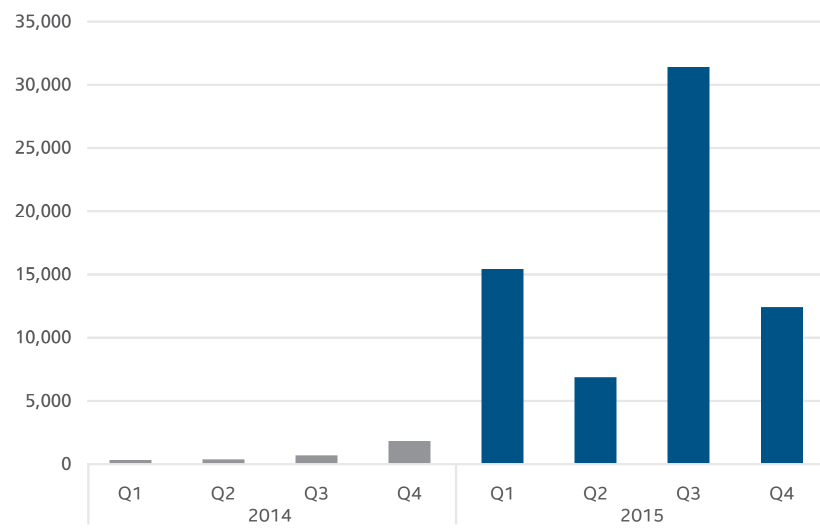


Source: McAfee Labs, 2016.

Share this Report

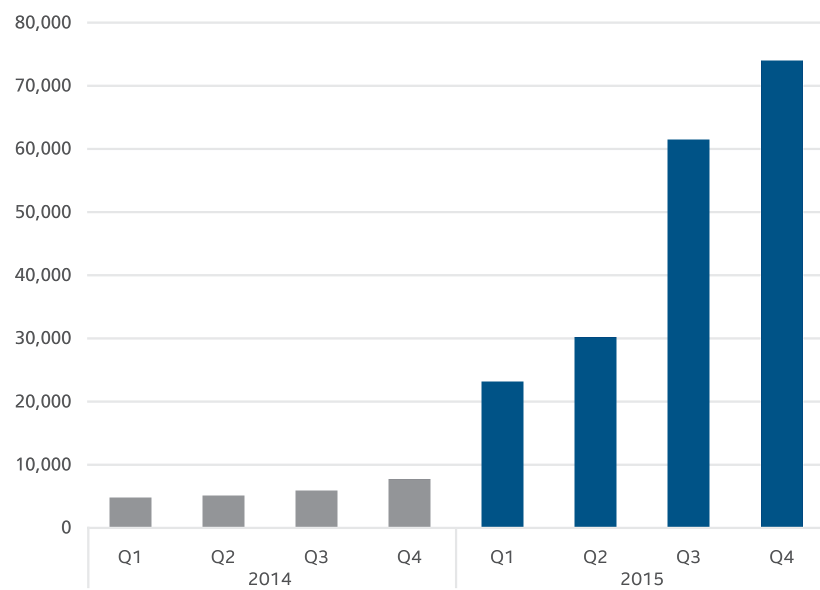
The number of new Mac OS malware samples is quite small and is highly influenced by just a few malware families.

New Mac OS Malware



Source: McAfee Labs, 2016.

Total Mac OS Malware



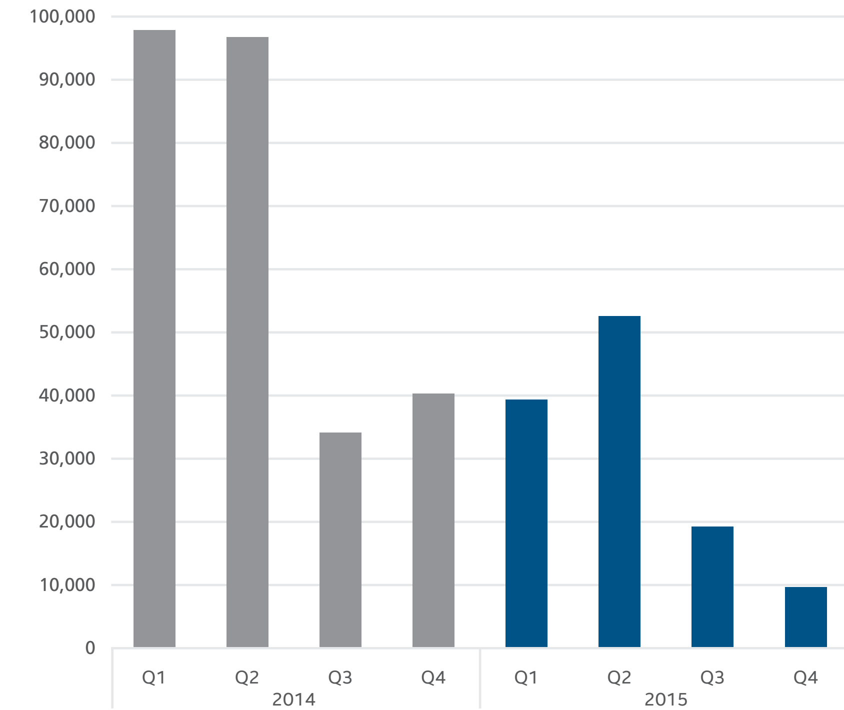
Source: McAfee Labs, 2016.

Share this Report

The number of new rootkit malware samples dropped precipitously in Q4, continuing a long-term downward trend in this type of attack. We believe the trend, which started in Q3 2011, is driven by ongoing customer adoption of 64-bit Intel processors coupled with 64-bit Microsoft Windows. These technologies include such features as Kernel Patch Protection and Secure Boot, which together protect against rootkit malware.

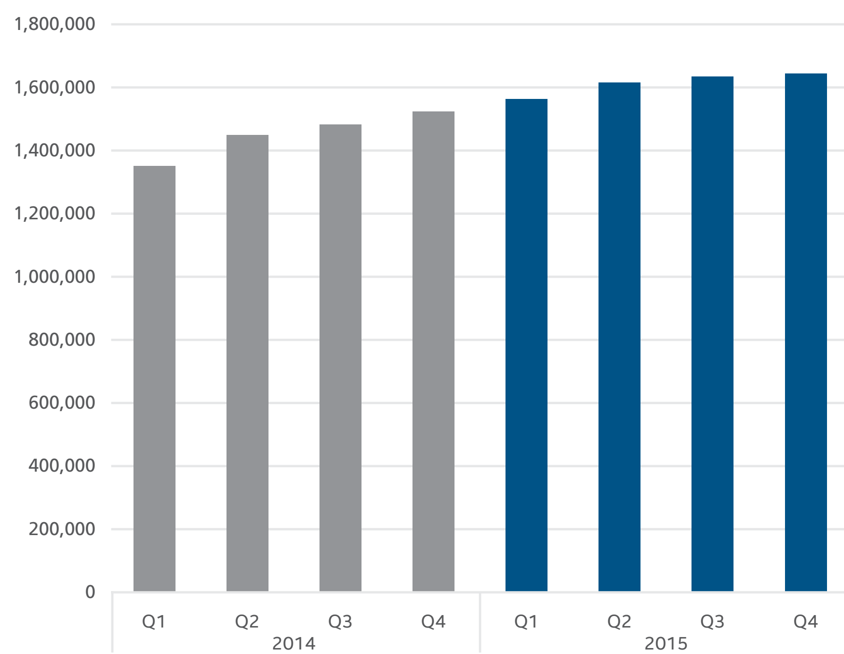
Because we do not expect rootkit malware to be significant in the near future, this is the last quarter in which we will report rootkit malware sample data. Of course, McAfee Labs will continue to monitor rootkit malware and we will resume our reporting should it again become significant.

New Rootkit Malware



Source: McAfee Labs, 2016.

Total Rootkit Malware

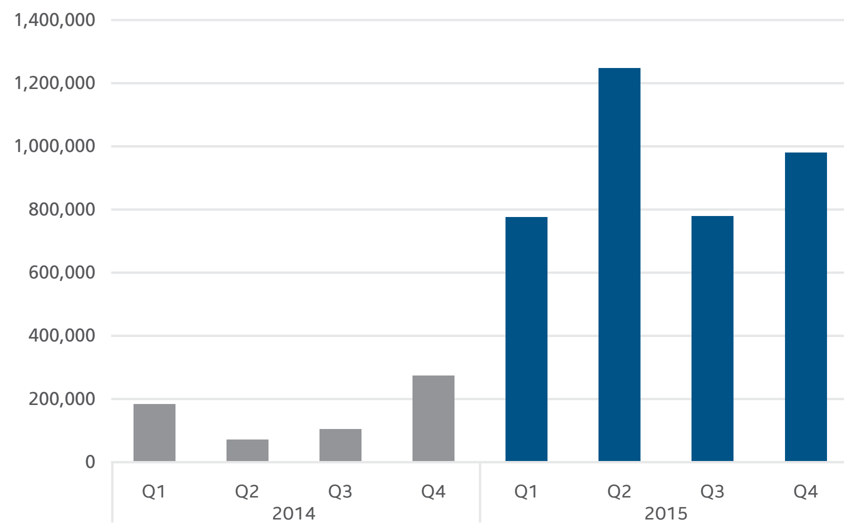


Source: McAfee Labs, 2016.

Share this Report

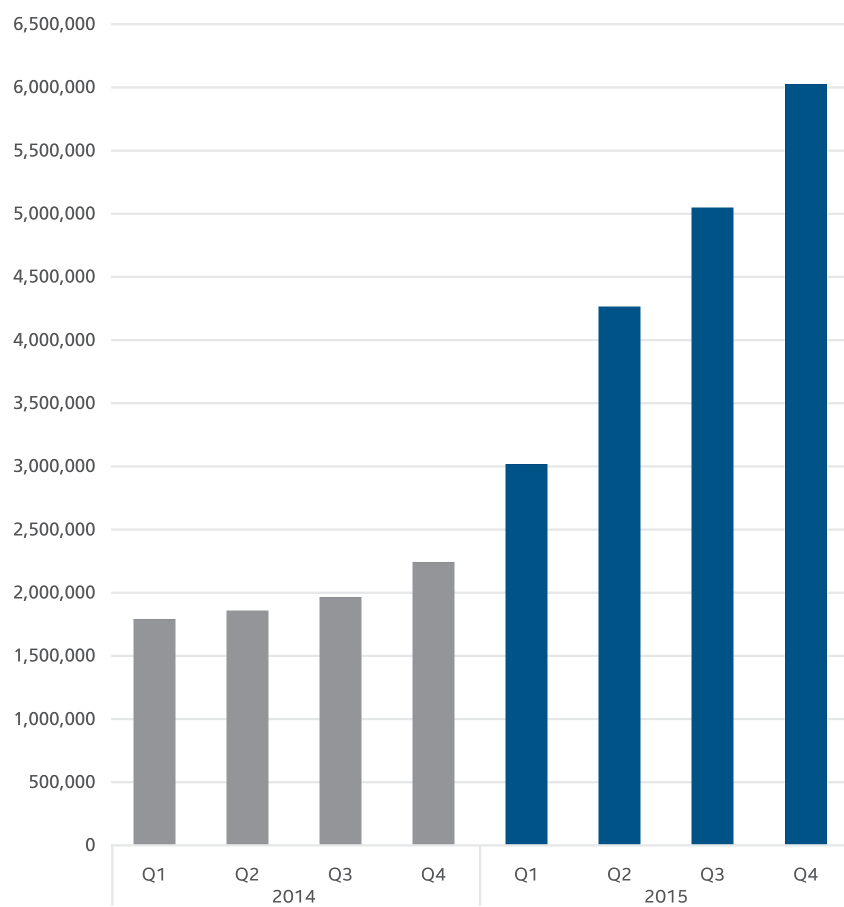
We saw a 26% increase in new ransomware samples in Q4 2015. The reason? Open-source ransomware code (for example, Hidden Tear, EDA2) and ransomware-as-a-service (Ransom32, Encryptor) make it simpler to create successful attacks. TeslaCrypt and CryptoWall 3 campaigns also continue. And as we detailed in the *McAfee Labs Threats Report: May 2015*, ransomware campaigns are financially lucrative with little chance of arrest, so they have become quite popular.

New Ransomware



Source: McAfee Labs, 2016.

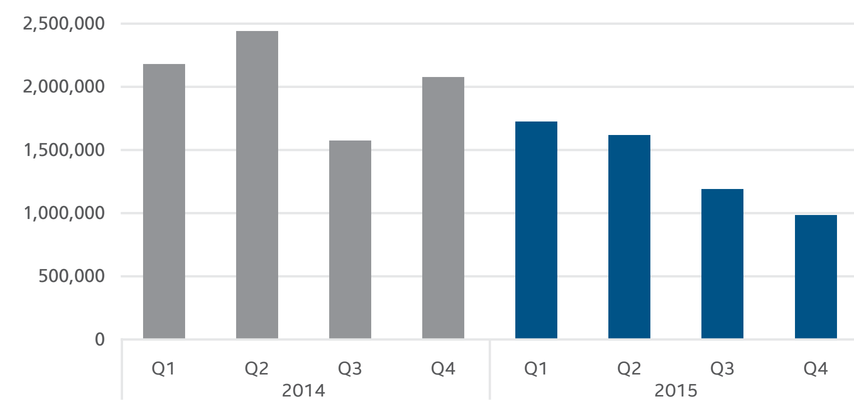
Total Ransomware



Source: McAfee Labs, 2016.

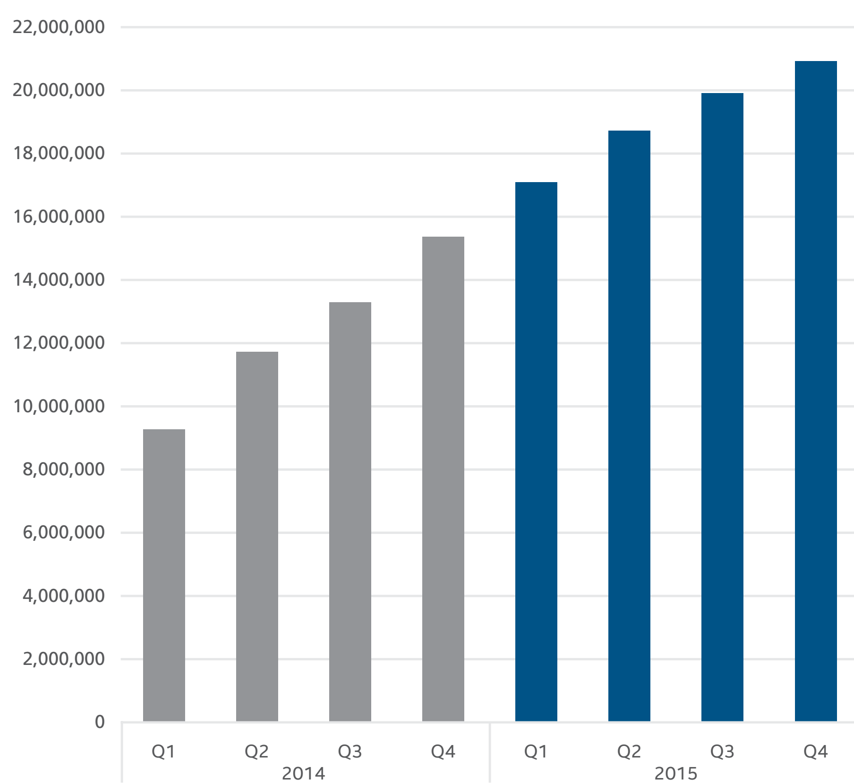
The number of new malicious signed binaries has dropped each quarter for the past year, in Q4 2015 reaching the lowest level since Q2 2013. McAfee Labs postulates that as businesses migrate to stronger hashing functions, older certificates with significant presence in the dark market are either expiring or being revoked. Also, technologies such as Smart Screen (part of Microsoft Internet Explorer but moving to other parts of Windows) represent additional tests of trust that might make the signing of malicious binaries less beneficial to malware authors.

New Malicious Signed Binaries



Source: McAfee Labs, 2016.

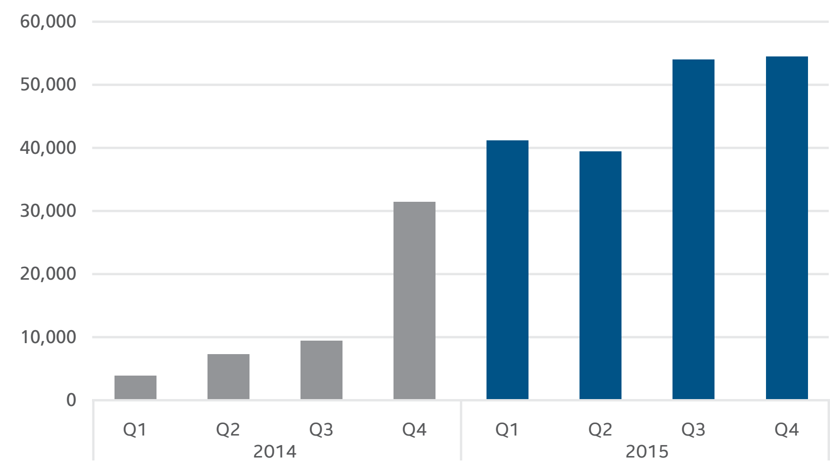
Total Malicious Signed Binaries



Source: McAfee Labs, 2016.

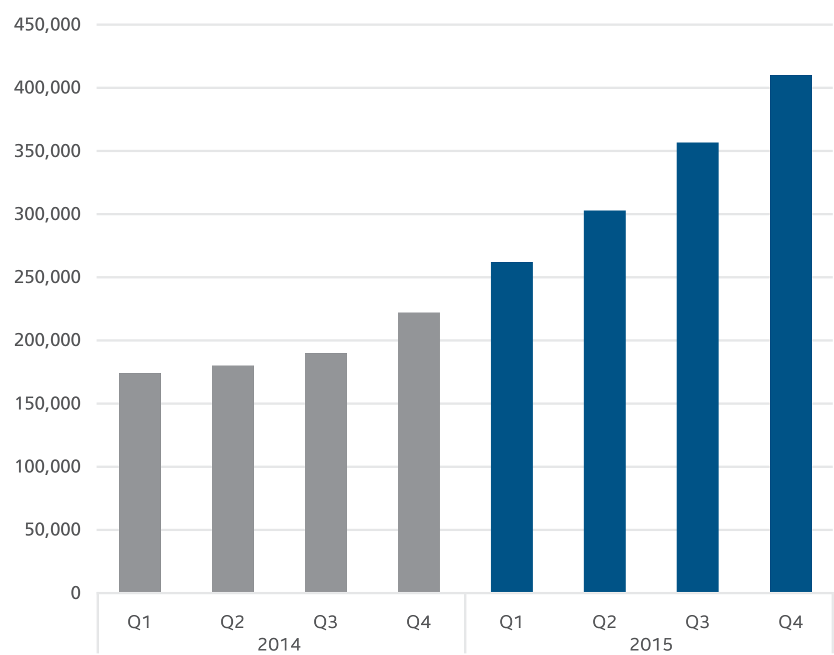
Share this Report

New Macro Malware



Source: McAfee Labs, 2016.

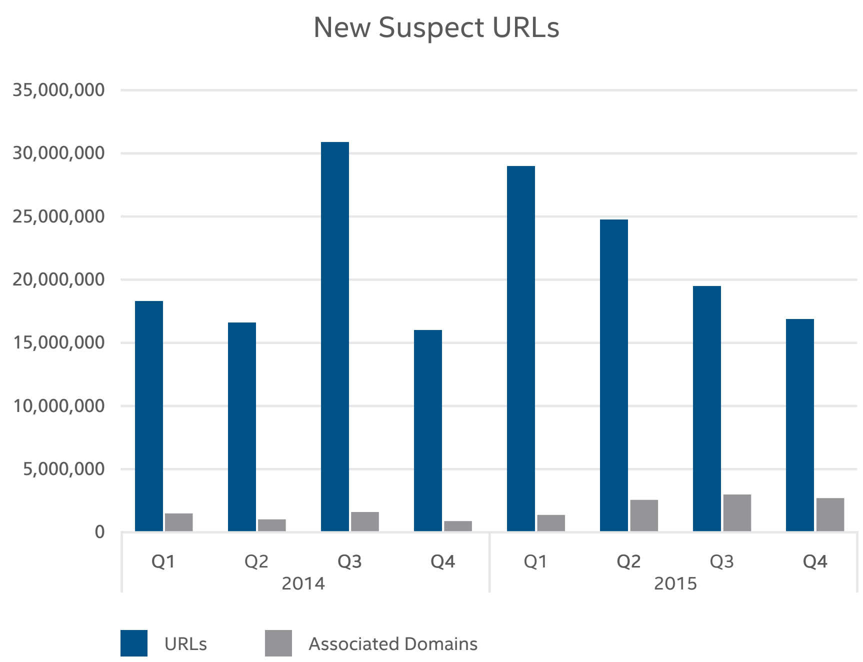
Total Macro Malware



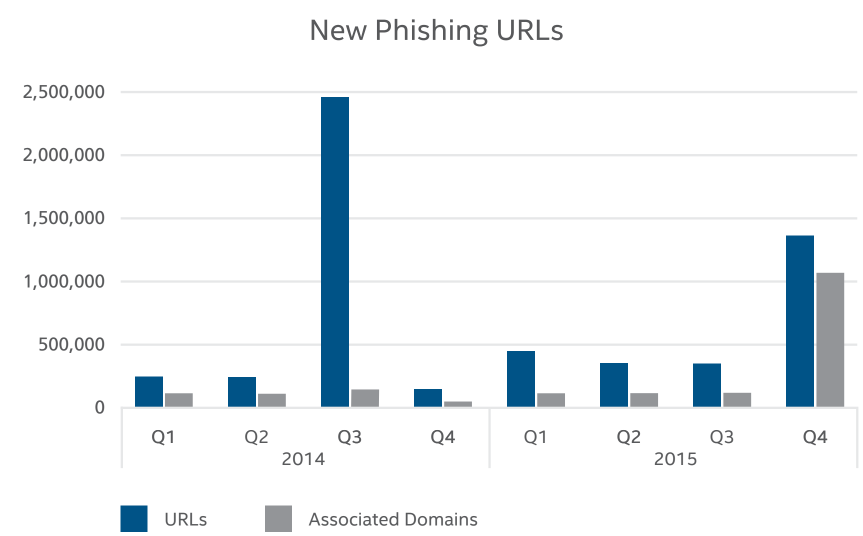
Source: McAfee Labs, 2016.

Share this Report

Web Threats



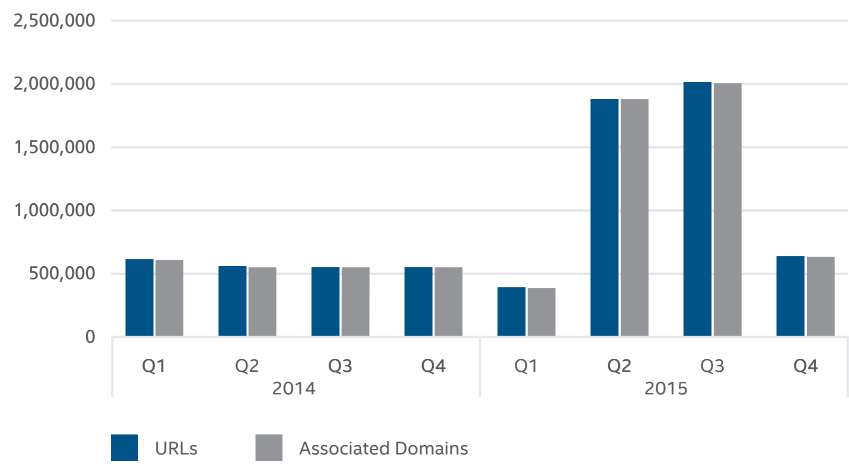
Source: McAfee Labs, 2016.



Source: McAfee Labs, 2016.

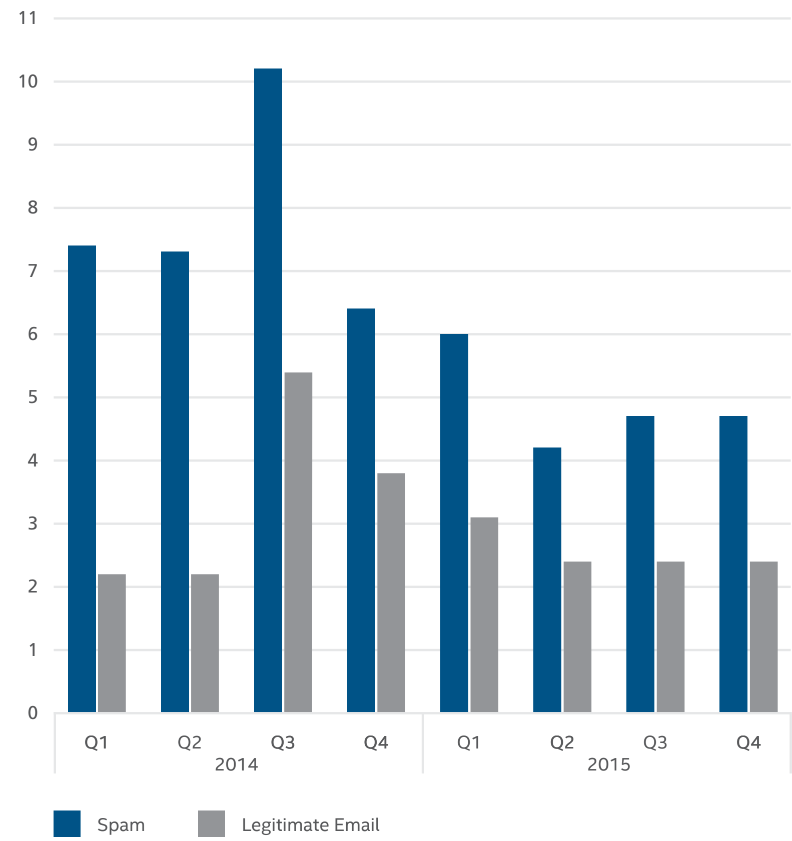
Share this Report

New Spam URLs



Source: McAfee Labs, 2016.

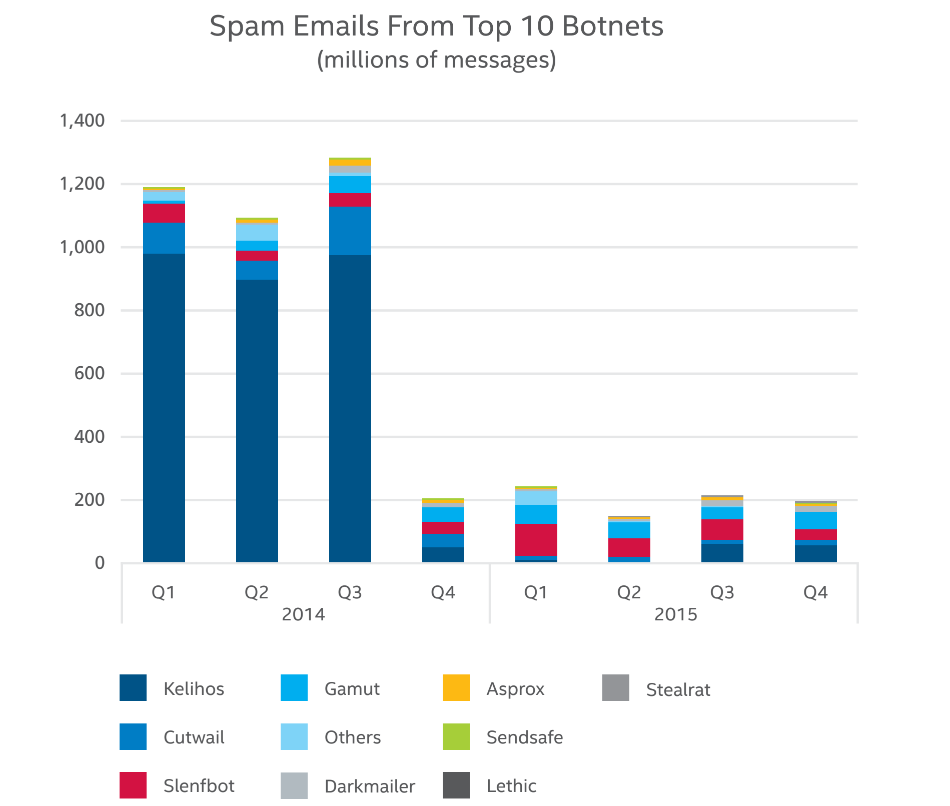
Global Spam and Email Volume
(trillions of messages)



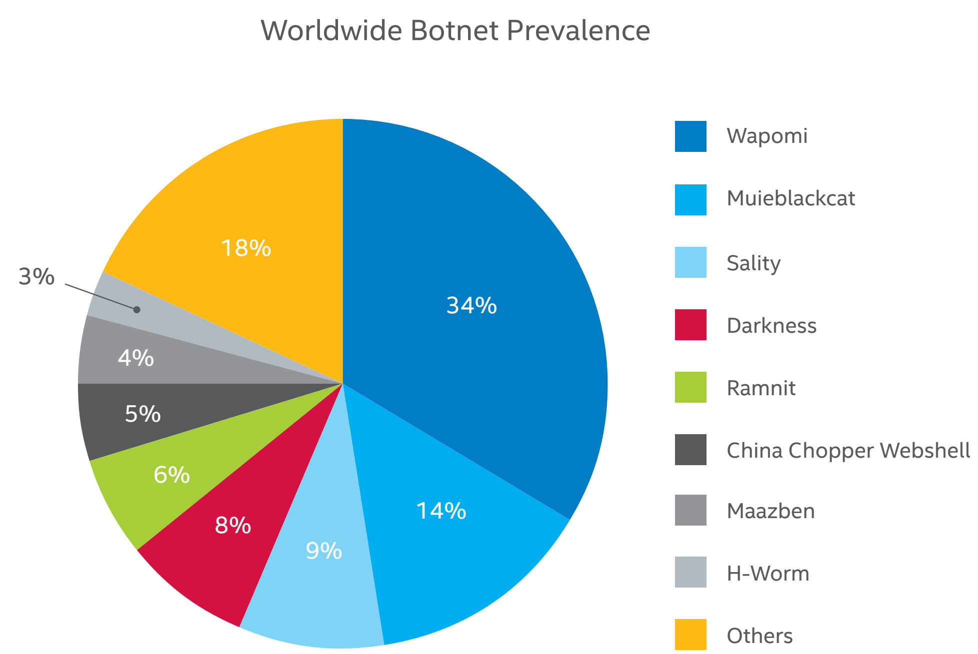
Source: McAfee Labs, 2016.

Share this Report

The Kelihos botnet held the top position during Q4, reaching about 95% of its Q3 volume. Alongside its well-known pharmaceutical spam, Kelihos took on another flavor by targeting Chinese recipients with "job offer" themed campaigns. Lethic botnet volumes increased by 60% during Q4, primarily with campaigns pushing knock-off designer wristwatches.



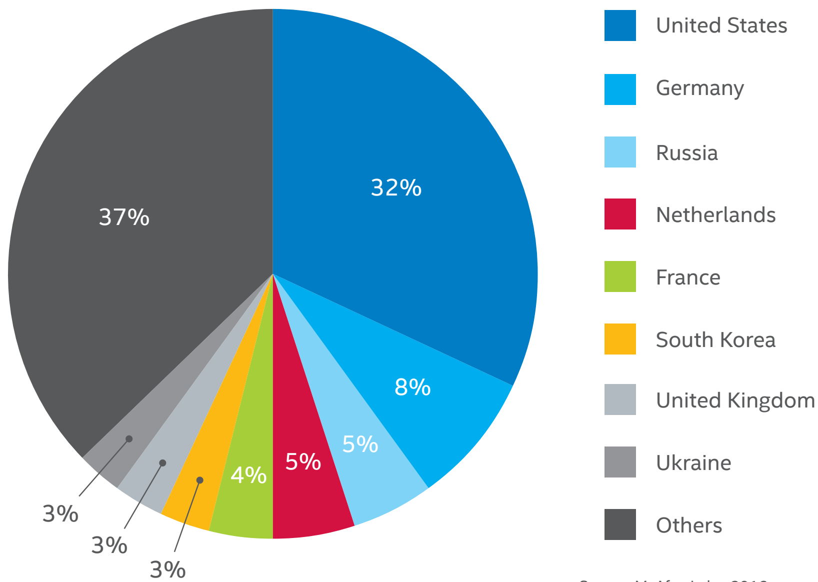
Source: McAfee Labs, 2016.



Source: McAfee Labs, 2016.

Share this Report

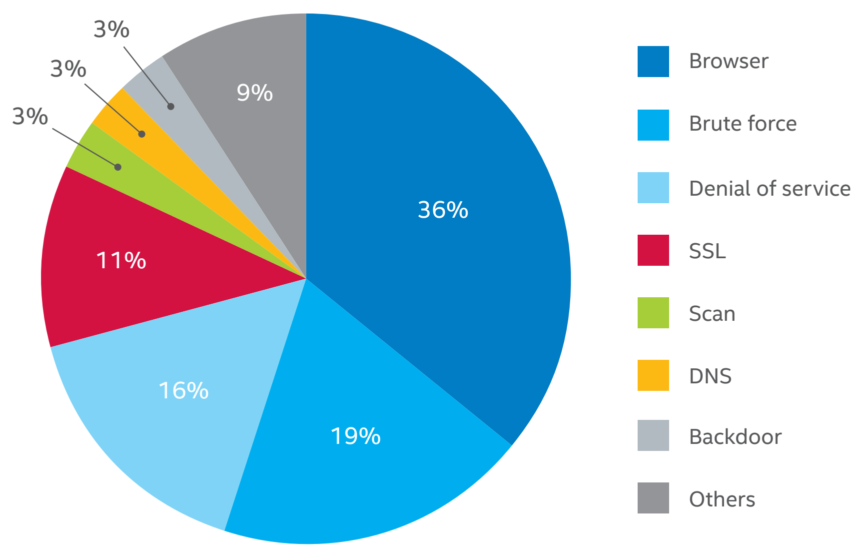
Top Countries Hosting Botnet Control Servers



Source: McAfee Labs, 2016.

Network Attacks

Top Network Attacks



Source: McAfee Labs, 2016.

Share this Report

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

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

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