FireEye
SECURITY REIMAGINED

SPECIAL REPORT

MAGINOT REVISITED:

More Real-World Results from Real-World Tests

SECURITY REIMAGINED

CONTENTS

EXECUTIVE SUMMARY

Attackers are bypassing conventional security deployments almost at will, breaching systems in a wide swath of industries and geographies. That's the stark conclusion of new data gathered by more than 1,600 FireEye network and email sensors deployed in real-world networks. Following up on our May 2014 report, "Cybersecurity's Maginot Line: A Real-World Assessment of the Defense-in-Depth Model," we compare data from the original Maginot report to new data gathered in the ensuing months.

Installed behind other security layers, the FireEye sensors offered a unique vantage point from which to gauge other security tools. Any threat observed by FireEye in the study had passed through all other security defenses.

The new data reaffirms our initial findings. It shows attacks getting through multiple layers of conventional defense-in-depth tools in the vast majority of deployments.

The new data also allows us to see trends for the first time. We saw marked increases in attacks using advanced malware[1] within the following sectors:

These industries saw a notable jump in the percentage of systems compromised during the study:

RETAIL
5% increase
(100 percent of systems breached)

HEALTHCARE AND PHARMACEUTICALS
4% increase
(100 percent of systems breached)

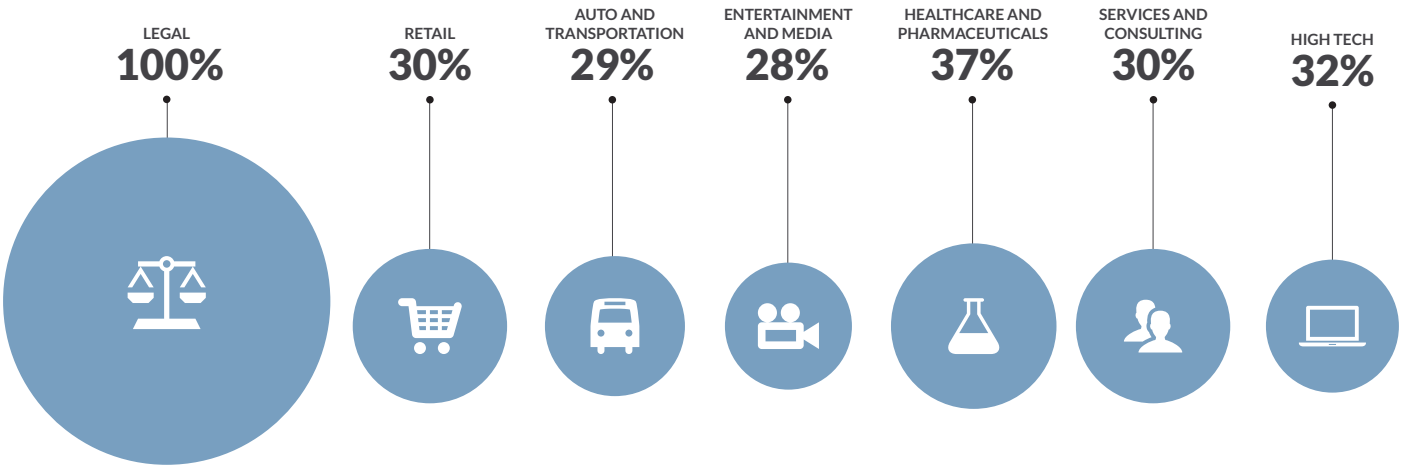
Across all industry segments, 96 percent of systems were breached on average. And 27 percent of those breaches involved advanced malware.

Given the widespread failings of conventional security deployments, organizations must consider a new approach to securing their IT assets.

They need to move away from passive, poorly integrated defenses that provide a fragmented view of threats and cannot connect the dots during advanced attacks. They need a tightly integrated, nimble architecture that enables big-picture vigilance.

Today's security teams can't afford to passively wait for attacks. Instead, they should take a lean-forward approach that actively hunts for new and unseen threats.

We call this approach FireEye Adaptive Defense.™



[1] For brevity, this report uses the term "advanced malware" to describe tools consistent with those used in advanced persistent threat (APT) attacks, even if those tools are widely used by other kinds of attackers.

BACKGROUND:

In May 2014, FireEye and Mandiant, a FireEye company, published "Cybersecurity's Maginot Line: A Real-World Assessment of the Defense-in-Depth Model." The first-of-its-kind study examined data from more than 1,200 security deployments in 63 countries across more than 20 industries.

The results were a startling indictment of conventional security architectures. In the vast majority of networks, cyber threats had slipped through all layers of organizations' defense-in-depth deployments.

In the first report, we likened this security gap to France's famed Maginot Line—an impressive but ultimately futile defense line built in the run-up to World War II to stave off a German invasion. In the same way, the cyber security industry has built up a complex, multilayered defense architecture that is doing little to stop a new generation of threats.

Unlike typical security lab tests, which assess security tools against precisely selected malware samples in highly controlled settings, this study analyzed data in real-world networks. It used data generated by 1,614 appliances in proof-of-value (PoV) trials of FireEye network and email appliances. Installed behind other security layers, these trial deployments offered a unique vantage point from which to gauge other security tools. Any threat observed by FireEye in the study had passed through all other security defenses that were supposed to be protecting an organization's network.

THE UPSHOT:

Despite the billions of dollars poured into conventional defenses every year, attackers are compromising networks almost at will. It doesn't matter what vendor or combination of typical defense-in-depth tools an organization has deployed. And it doesn't matter how well these tools performed in lab tests. Real-world attackers are bypassing them all.

HERE'S A SAMPLE OF WHAT WE FOUND IN THE FIRST REPORT:

97%

of organizations in the study were breached during the test period.

>1/4

More than a fourth of all organizations experienced events consistent with tools and tactics employed by known advanced persistent threat (APT) actors.

Three-fourths of organizations had active command-and-control communications, indicating that attackers had control of the breached systems and were possibly already receiving data from them.

>1/week

Even after an organization was breached, attackers attempted to compromise the typical organization more than once per week on average.

NEW DATA, SAME OUTCOME

Since that report, we have continued to collect data from PoV deployments to validate our initial findings and identify trends over time. The deployments comprised organizations that had installed FireEye equipment for testing but were not yet protected by the FireEye platform.

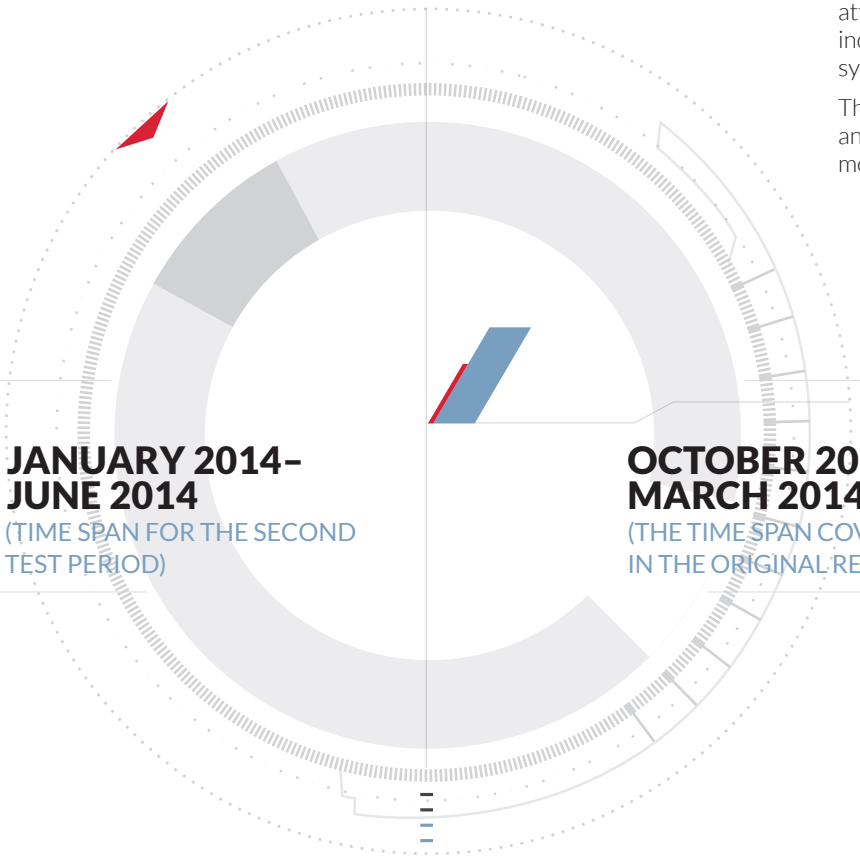
We examined data from 1,214 security deployments over two overlapping six-month test periods:

This report highlights changes we saw in the second test period versus the first. The new data confirms our original conclusions. Attackers continue to bypass conventional security tools, breaching the vast majority of security architectures. And roughly a quarter of those breached systems encountered tools and techniques consistent with known APT attackers.

The new data also allows us to see trends for the first time. While the overarching tenor hasn't changed since the original report, many of the details have.

First, we saw marked increases in advanced attacks targeting several sectors. Second, several industries saw a notable jump in the percentage of systems compromised during the study.

The following sections outline both of these shifts and detail the advanced malware families used most frequently in these segments.



JANUARY 2014–JUNE 2014
(TIME SPAN FOR THE SECOND TEST PERIOD)

OCTOBER 2013–MARCH 2014
(THE TIME SPAN COVERED IN THE ORIGINAL REPORT)

The new data confirms our original conclusions. Attackers continue to bypass conventional security tools, breaching the vast majority of security architectures.

WHAT IS APT MALWARE, AND WHY SHOULD I CARE?

FireEye tracks countless malware variants all over the world. But we pay special attention to those commonly used in APT attacks. In the FireEye naming convention, these are identified with "APT" in the subtype. For example, the "APT" in the widely used Gh0stRAT malware family is expressed as BACKDOOR.APT.GH0STRAT.

APT attackers receive direction and support from a national government. Whether their mission is to steal data, disrupt operations, or destroy infrastructure, these threat actors tenaciously pursue their goal using a wide range of tools and tactics.

The presence of an APT-linked malware variant in your system does not always mean that you are in the crosshairs of an APT actor. That's because APT attacks often employ widely available tools to camouflage their actions or for simple convenience. In other words, it could be anyone. Figuring out who is using the malware usually requires more context than the malware alone.

Even so, your security team should pay close attention when their security tools detect malware linked to previous APT attacks.

While the malware doesn't always mean an APT actor is targeting you, the possibility is worth probing further. APT actors' motives aren't always clear. You might have data that APT actor thinks is worth stealing—or connections to other people and entities that have it—and not realize it.

Moreover, the "APT" label often indicates that the malware itself is advanced. Even in the hands of a non-APT attacker, the malware could prove difficult to analyze and resolve. Detecting it and responding quickly is critical.

In this report, we highlight some of the top malware detected within industry verticals that saw a spike in APT-related malware, including how it works and its business impact.

For brevity, this report uses the term "advanced malware" to describe tools consistent with those used in APT attacks, even if those tools are widely used by other kinds of attackers.

Figuring out who is using the malware usually requires more context than the malware alone. Even so, your security team should pay close attention when their security tools detect malware linked to previous APT attacks.

LARGEST INCREASES IN COMPROMISES

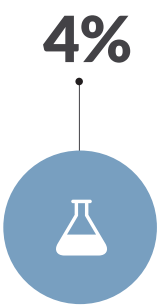
While the percentage of compromised systems held steady overall, retail and healthcare sectors saw substantial spikes.

RETAIL

The number of breached systems in the retail sector rose more than 5 percent. All 58 deployments in our sample had been breached by the end of the study—17 percent of those by advanced malware.

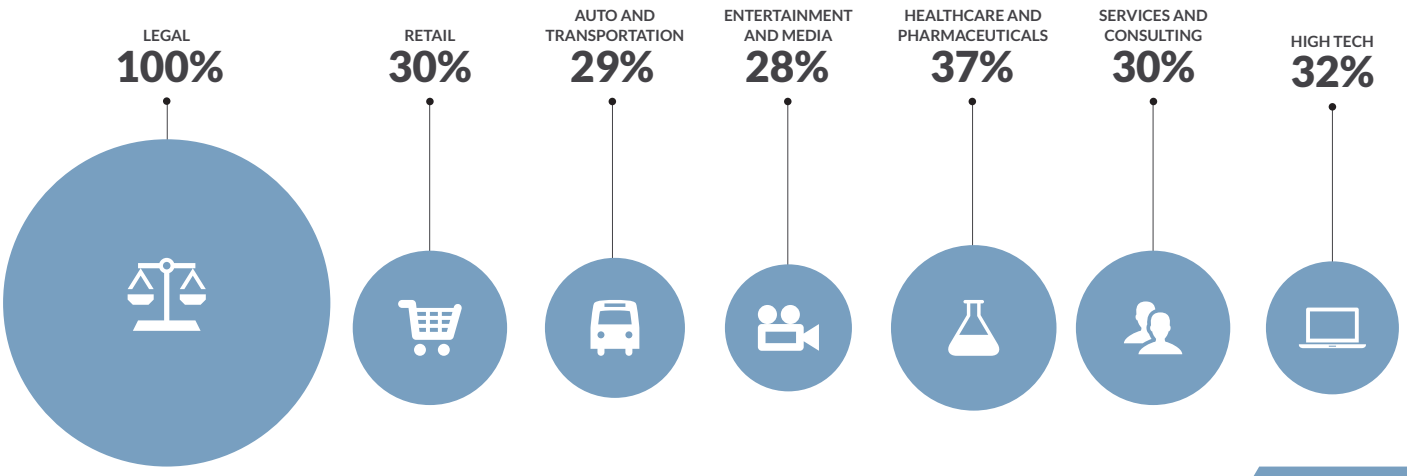
HEALTHCARE AND PHARMACEUTICALS

The number of breached systems among healthcare and pharmaceutical firms rose more than 4 percent. All 54 deployments in our sample had been breached by the end of the study—more than 37 percent of those by advanced malware.



LARGEST INCREASES IN ADVANCED MALWARE ACTIVITY

The overall percentage of breaches that involved advanced malware held steady at about 27 percent. Several industry segments saw double- and even triple-digit jumps in advanced malware activity.



LEGAL

Among law firms, the percentage of breaches involving advanced malware doubled from the previous test period to 10 percent. Although the vast majority of breaches among legal firms still did not involve advanced malware in the most recent test period, the 100 percent increase was by far the largest of any industry segment.

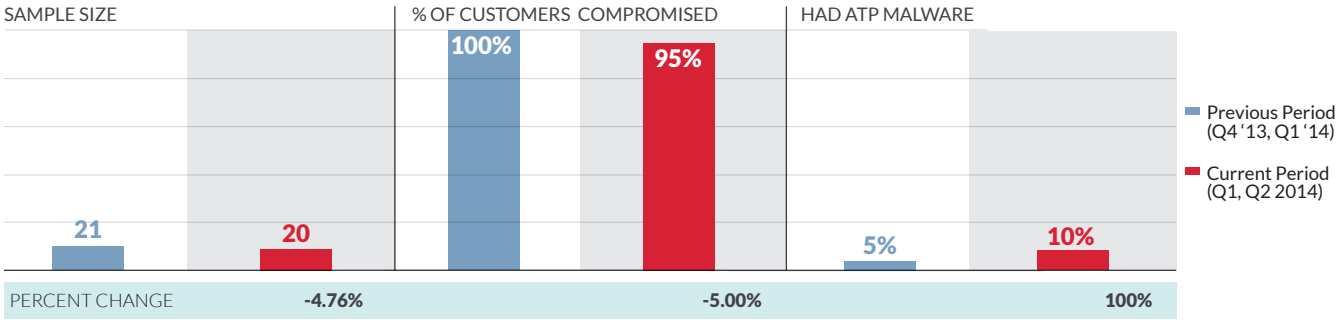
The primary culprit was **TROJAN.APT.PINGBED**, with **TROJAN.APT.HEARTBEAT** a distant second.

100% INCREASE IN ADVANCED MALWARE

First spotted in August 2011, Pingbed targets Windows-based PCs and has appeared mostly in the U.S. Typically, attackers trick users into opening or unzipping malicious PDF or Microsoft Word files. Once opened, the Trojan downloads, installs, and executes malicious files. It can also do the following:

- Configure delays—an advanced sandbox-evasion method
- Gather information about running processes on the infected PC—letting attackers know about vulnerable software on the PC
- Kill running processes on the PC, including security measures
- Execute command lines

COMMON ATTACK VECTORS are through email and the web. Attacks using Pingbed typically tamper with users' web browsers and steal data, including legal strategies, confidential information on clients and opponents. Attacks of this nature can complicate victims' cases and create additional legal problems.



RETAIL

Recent breaches of big-name retailers have helped bring cyber security into the mainstream, touching millions of customers. So perhaps it comes as no surprise that the number of breaches in the sector involving advanced malware rose 30 percent, representing 17% of all retail attacks.

BACKDOOR.APT.GH0STRAT, one of the most popular malware variants in recent months across all sectors, appeared most frequently among breached retail systems. We also spotted **TROJAN.APT.SIDEBARDLL**, **TROJAN.APT.HANGOVER**, **BACKDOOR.APT.1PHP**, though far less frequently.

DATA THEFT IN AISLE 9: MALWARE THREATS TO RETAILERS

(ADAPTED FROM A BLOG POST BY NART VILLENEUVE, FIREEYE SENIOR THREAT INTELLIGENCE RESEARCHER)

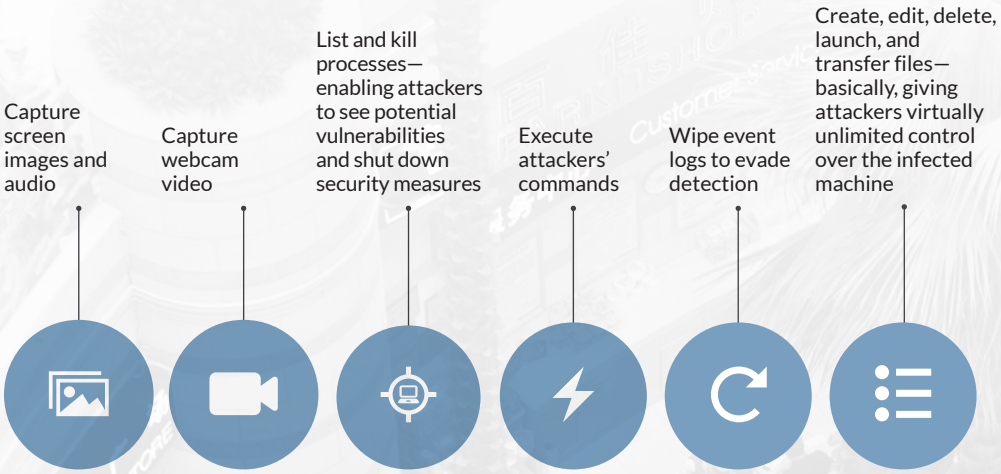
Since 2013, we have seen a sharp increase in malware threats focused on point-of-sale (POS) systems.

The reason is simple: retailers have a lot of valuable data residing in retailers' networks, and lots of criminals want it.

(Continued on page 19.)

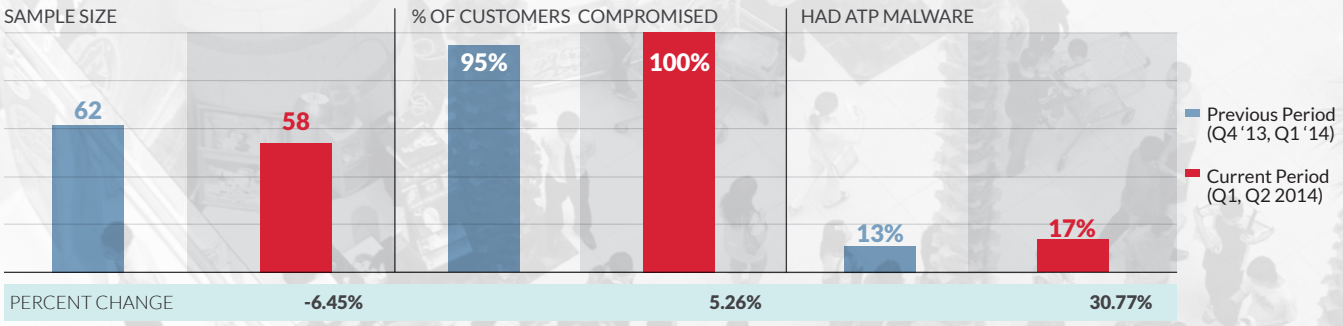
30% INCREASE IN ADVANCED MALWARE

First spotted in August 2012, Gh0stRAT gives attackers wide control over infected systems. The backdoor malware can do the following:



COMMON ATTACK VECTORS ARE through email and the web. Attacks using Gh0stRAT typically trick users into opening a malicious document. From there, the backdoor tampers with users' web browser and steals data—especially credit card numbers. Despite headlines of big breaches at U.S. retailers, those in South Korea were breached most often.

The business impact of these breaches include tangible costs such as lost sales when wary customers avoid breached retailers and having to notifying affected customers.



AUTO AND TRANSPORTATION

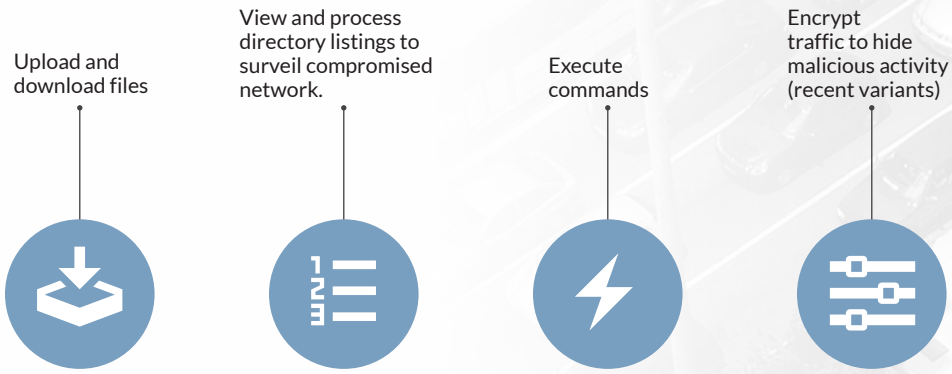
Although breaches of auto and transportation companies haven't generated many headlines, we saw a 29 percent jump in breaches using advanced malware—a jump nearly as great as the increase we saw in retail. Perhaps more alarming: a full 40 percent of breached systems were infected with advanced malware, one of the highest percentages of any industry.

The most common malware spotted on infected systems in this sector was **BACKDOOR.APT.IXESHE.** We also saw **TROJAN.APT.SHIQIANG**, **BACKDOOR.APT.LECNA**, and **BACKDOOR.APT.HUPIGON**, though far less frequently.

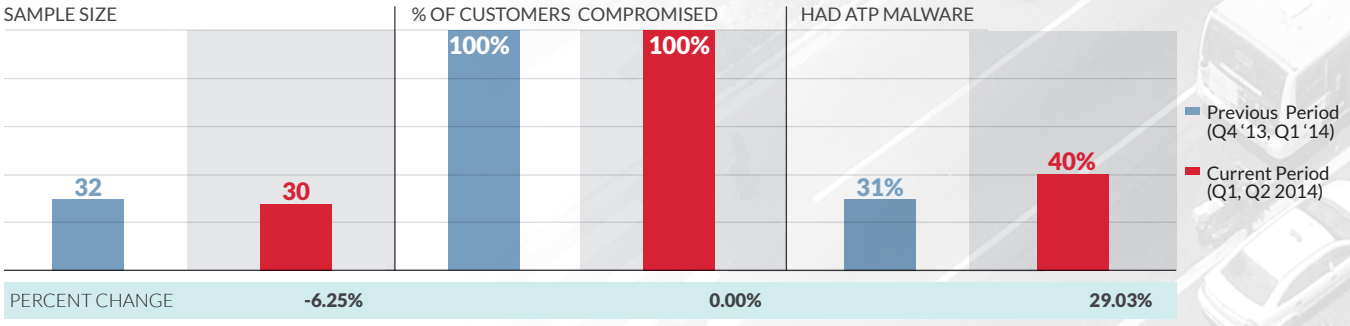
29 % INCREASE IN ADVANCED MALWARE

First seen in November 2011, Ixeshe (pronounced "eye-sushi") tricks users into opening a weaponized document, typically a PDF. Once opened, it extracts passwords from Microsoft Explorer's protected storage to authenticate itself to proxy servers. The malware can do the following:

Ixeshe sets up command-and-control (CnC) servers within other compromised networks to minimize external traffic to suspicious IP addresses. This sleight-of-hand makes can make Ixeshe especially hard to detect.[1]



COMMON ATTACK VECTORS include email and web traffic. The malware appeared most frequently in attacks against U.S. entities. Its potential business impact includes theft of data and intellectual property. It can also harvest user credentials, leading to future attacks.



[1] Tim Wilson (*InformationWeek*). "New Advanced Persistent Threat, IXESHE, On The Rise." May 2012.

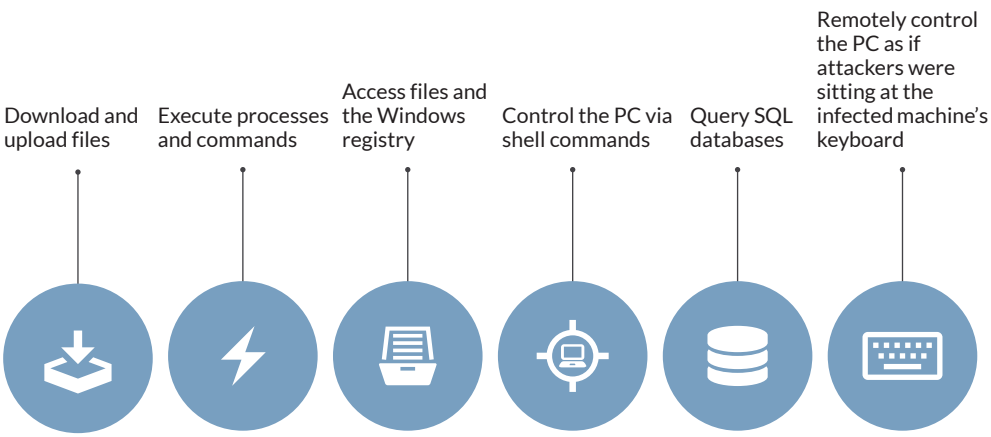
ENTERTAINMENT AND MEDIA

The concentration of breaches among entertainment and media companies involving advanced malware rose more than 28 percent, constituting about 18 percent of all breaches in this segment during the most recent test period.

The most common malware family was **BACKDOOR.APT.KABA. TROJAN.APT.SISPROC** and **BACKDOOR.APT.GH0STRAT** were a distant No. 2 and No. 3, respectively.

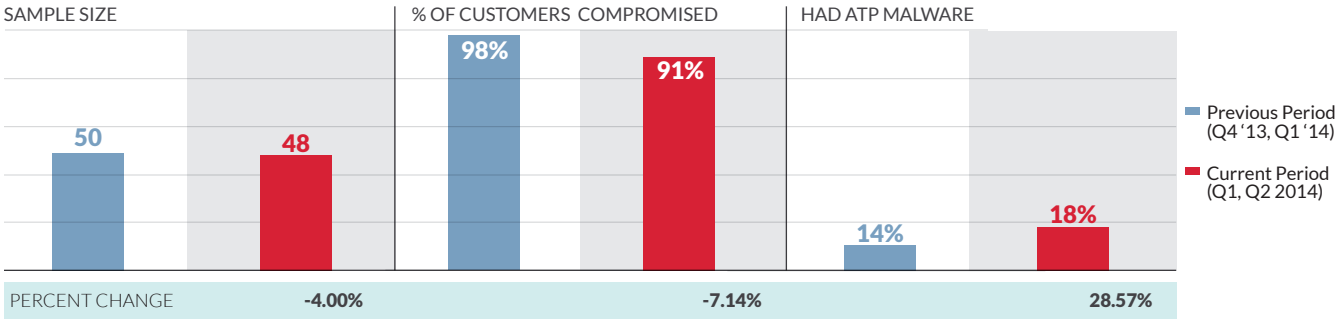
28% INCREASE IN ADVANCED MALWARE

Kaba, also known as PlugX, was first spotted in January 2012. The well-known remote-access tool (RAT) give attackers nearly full control of infected machines. Kaba can do the following:



COMMON ATTACK VECTORS include email and web traffic. In most cases, Kaba exploits a flaw in Microsoft Office. To avoid detection, Kaba loads the malicious executable into memory but never writes it to the disk, where a malware scanner might detect it.

U.S.-based entertainment firms were the biggest targets. Firms compromised by Kaba could lose intellectual property—everything from marketing plans to unreleased music, shows, and movies—and other valuable data.



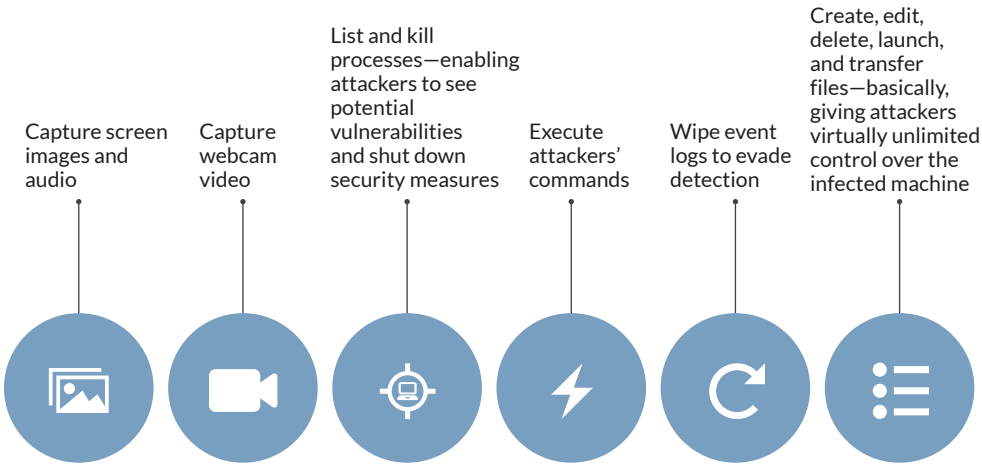
HEALTHCARE AND PHARMACEUTICALS

The percentage of systems in the healthcare and pharmaceutical industries with advanced malware rose more than 37 percent, constituting about 22 percent of all breaches in this segment during the most recent test period.

The most common malware was **BACKDOOR.APT.GH0STRAT**, followed by **TROJAN.APT.SISPROC** and **TROJAN.APT.MOLERAT.**

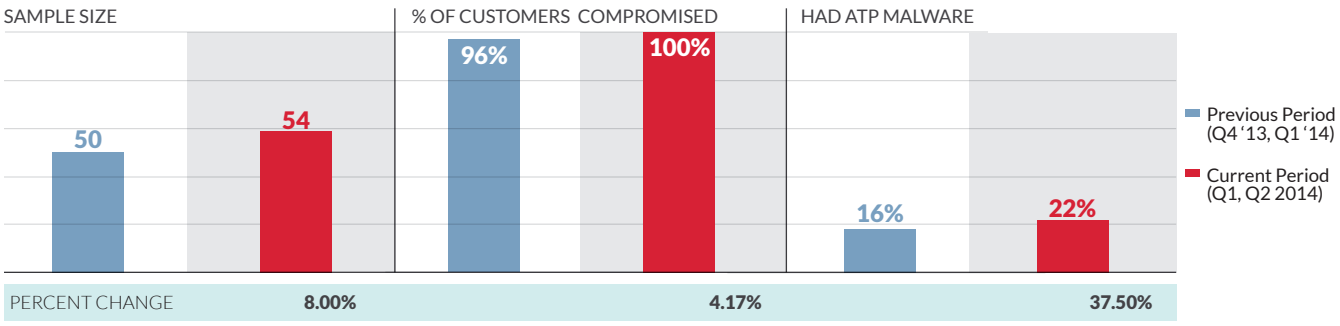
37% INCREASE IN ADVANCED MALWARE

As explained in "Retail" on page 3, Gh0stRAT is a popular RAT tool that gives attackers wide-ranging control of infected systems. Compromised system could lose anything from patient data to development plans and formulas for new drugs.



COMMON ATTACK VECTORS ARE through email and the web. Attacks using Gh0stRAT typically trick users into opening a malicious document. From there, the backdoor tampers with users' web browser and steals data—especially credit card numbers. Despite headlines of big breaches at U.S. retailers, those in South Korea were breached most often.

The business impact of these breaches include tangible costs such as lost sales when wary customers avoid breached retailers and having to notifying affected customers.



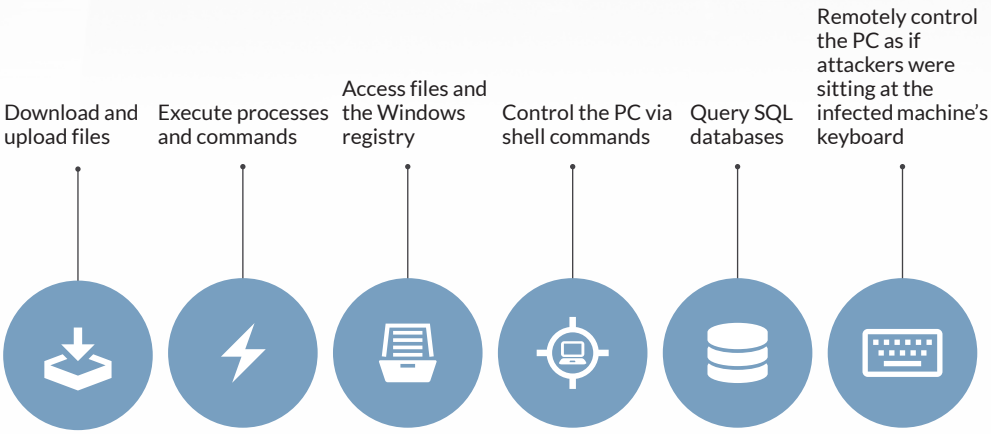
SERVICES AND CONSULTING

The concentration of advanced malware that breached services and consulting firms rose more than 38 percent, constituting nearly 30 percent of all breaches in this segment during the most recent test period.

The most common malware was **BACKDOOR.APT.KABA,** followed by **TROJAN.APT.HEARTBEAT** and **BACKDOOR.APT.POISONIVY.**

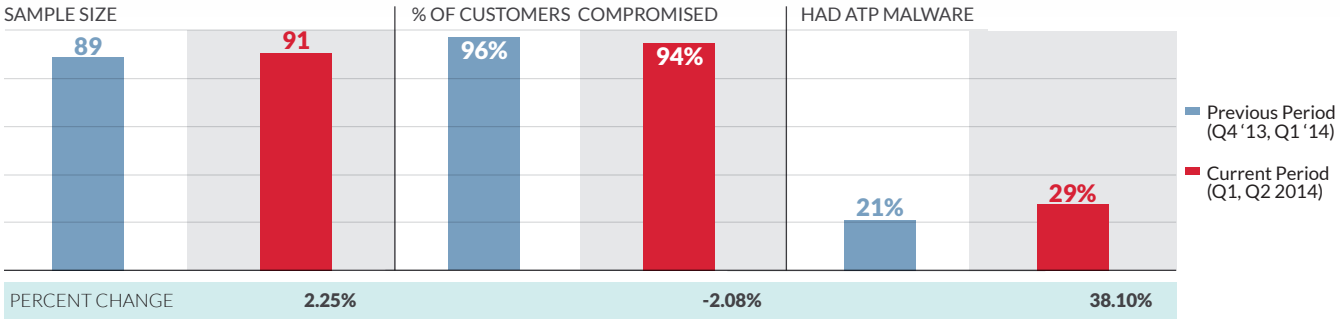
38% INCREASE IN ADVANCED MALWARE

Kaba, also known as PlugX, was first spotted in January 2012. The well-known remote-access tool (RAT) give attackers nearly full control of infected machines. Kaba can do the following:



COMMON ATTACK VECTORS include email and web traffic. In most cases, Kaba exploits a flaw in Microsoft Office. To avoid detection, Kaba loads the malicious executable into memory but never writes it to the disk, where a malware scanner might detect it.

In many cases attackers target services and consulting firms in order to steal information from their clients. For example information on M&A activity, negotiating tactics and legal strategies are frequent targets.



HIGH TECH

The concentration of advanced malware breaching high-tech firms rose nearly a third, constituting about 32 percent of all breaches in the most recent test period.

COMMON ATTACK VECTORS include email and web traffic. XtremeRAT has been used in many attacks by state-sponsored attackers and novice hackers alike. These include well-publicized attacks in the Middle East.2 But the malware appeared most frequently in breaches of U.S.-based entities.

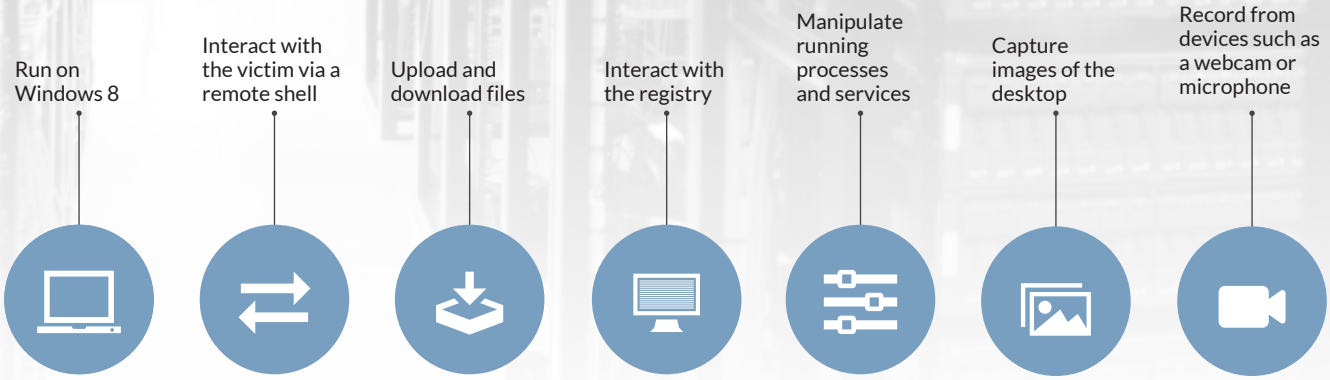
Given XtremeRAT's rich features and convenience, its potential business impact is hard to measure. In the wrong hands, the malware could be used in anything from stealing data to commercial spying.

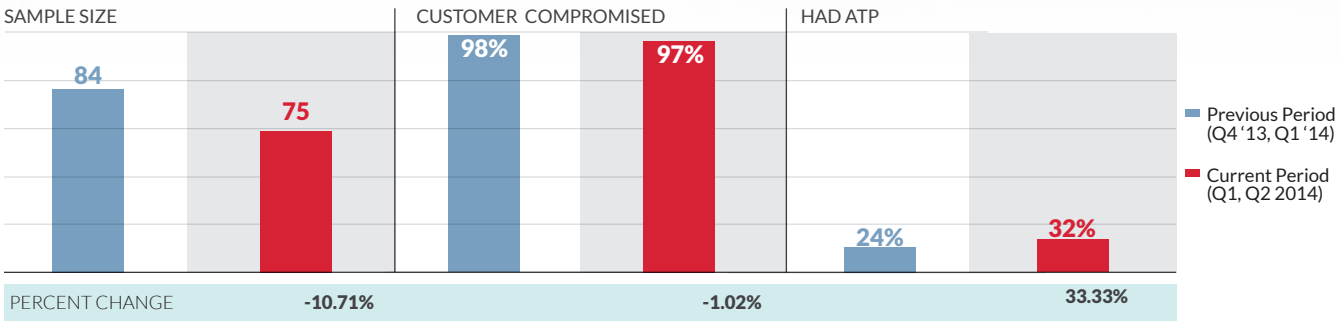
While the percentage of compromised systems held steady overall, retail and healthcare sectors saw substantial spikes.

The most common malware was **BACKDOOR.APT.XTREMERAT**, followed closely by **BACKDOOR.APT.3128CREDS** and **BACKDOOR.APT.HOUDINI.**

32% INCREASE IN ADVANCED MALWARE

XtremeRAT, first seen in November 2012, is an openly available (and highly versatile) RAT that can do the following:





[2] Nart Villeneuve and James T. Bennett (FireEye). "XtremeRAT: Nuisance or Threat?" February 2014.

HIGHEST CONCENTRATION OF ADVANCED MALWARE

Half of all agriculture firms were breached with advanced malware, the highest concentration of any segment. But our sample size was small, and the original test period did not have any deployments in this sector for comparison. The transportation segment was No. 2 with advanced malware in 40 percent of all breaches. Table 1 details advanced malware concentration across all industries in our sample.

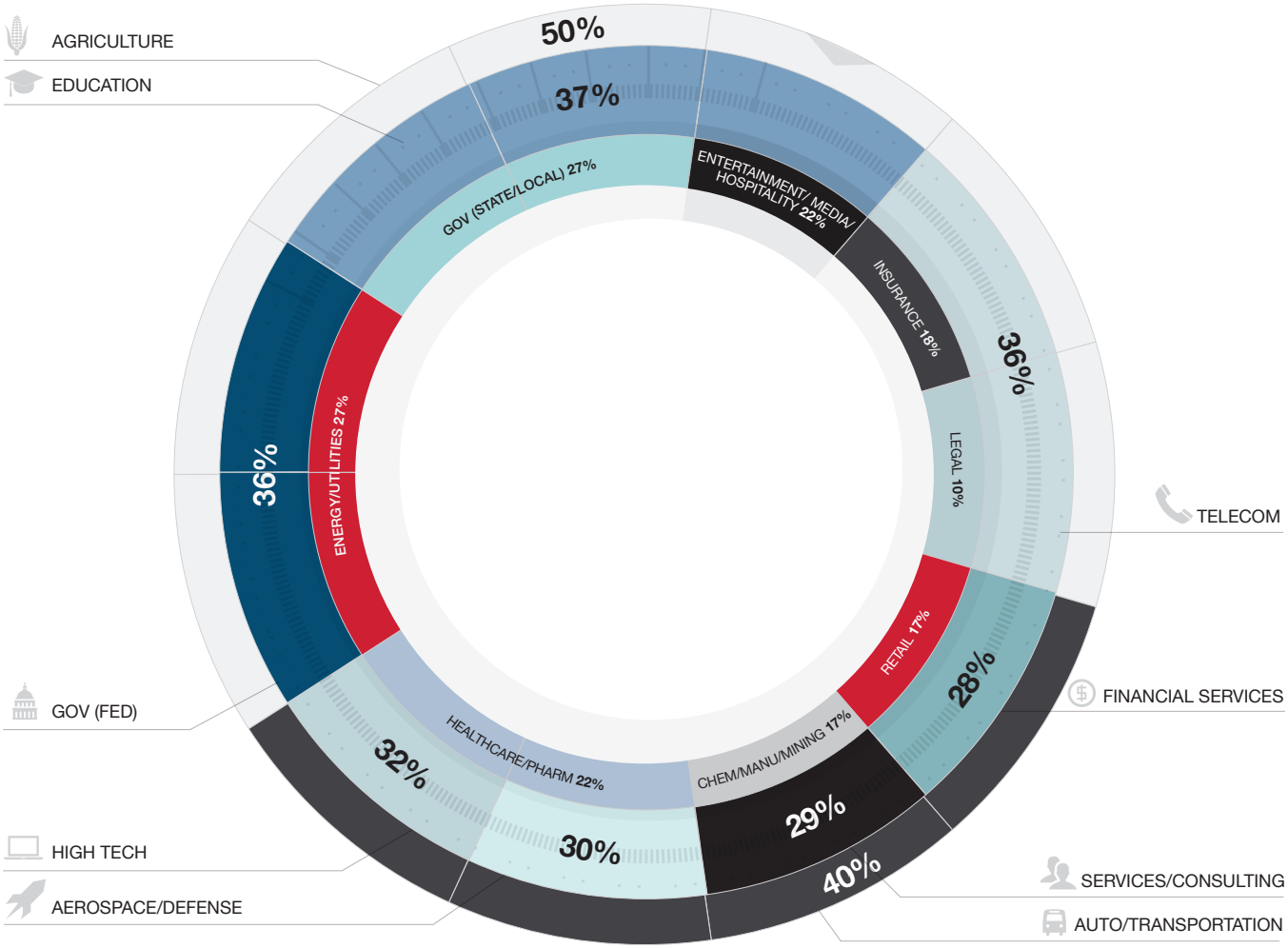


Table 1: Advanced malware concentration by industry

Had Advanced Malware					
Agriculture	50%	Aerospace/Defense	30%	Entertainment/Media/Hospitality	18%
Auto/Transportation	40%	Services/Consulting	29%	Insurance	18%
Education	37%	Financial Services	28%	Chem/Manu/Mining	17%
Gov (Fed)	36%	Energy/Utilities	27%	Retail	17%
Telecom	36%	Gov (State/Local)	27%	Legal	10%
High Tech	32%	Healthcare /Pharm	22%	Average	27%

HIGHEST CONCENTRATION OF BREACHES

As shown in Table 2, more than 96 percent of the deployments in our sample experienced a breach during our study. All of the deployments in agriculture, auto and transportation, education, and retail were breached. And at least 90 percent of the deployments in all other sectors were breached, with one notable exception.

A "mere" 76 percent of all aerospace and defense firms were breached. While the number is unacceptably high, it is significantly lower than other industries. One possible explanation: many firms in this sector, long a target of advanced state-sponsored attacks, have beefed up their cyber defenses. But as the data shows, most of these defenses continue to fail.

Table 2: Breaches by industry

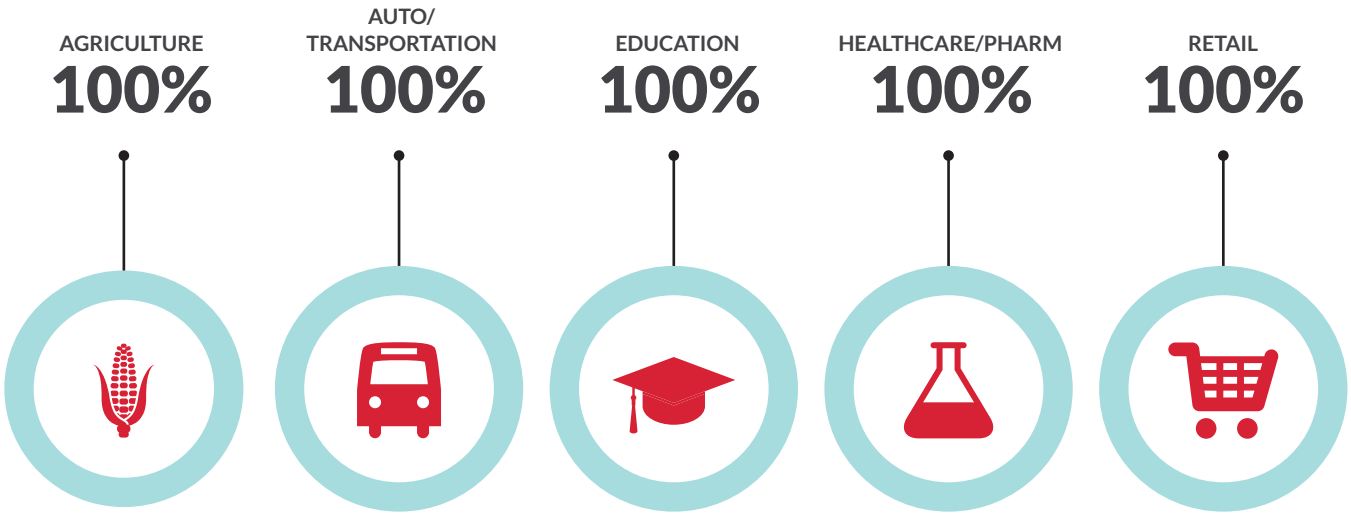
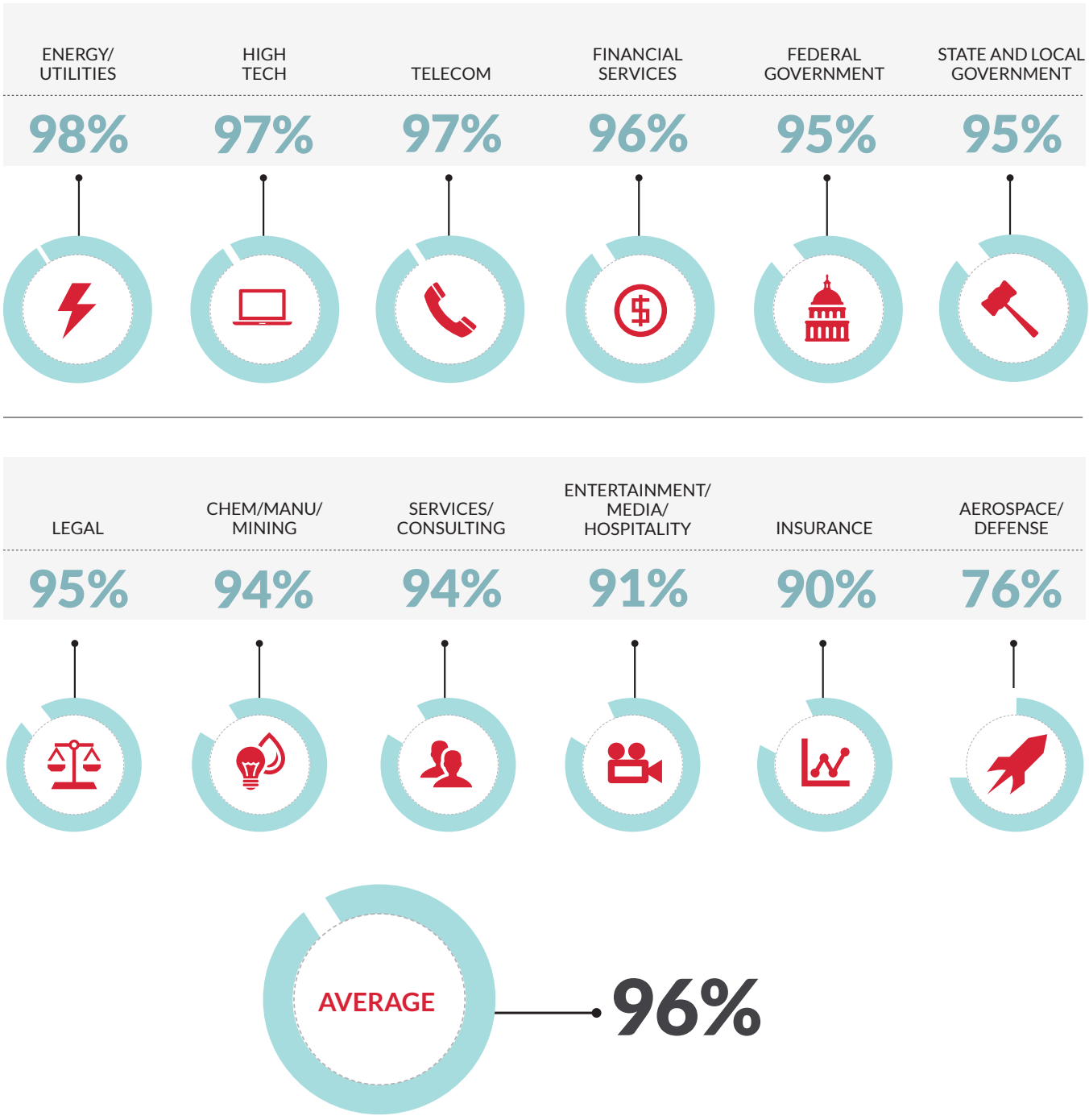


Table 2: Breaches by industry



DATA THEFT IN AISLE 9: MALWARE THREATS TO RETAILERS

(ADAPTED FROM A BLOG POST BY NART VILLENEUVE, FIREEYE SENIOR THREAT INTELLIGENCE RESEARCHER)

(Continued from Page 10)

Thriving underground markets and a cyber criminal ecosystem enable threat actors to craft and trade their wares. Here are some of the most common POS malware families and their similarities:

1 Backoff POS

Attacks involving Backoff were publicly disclosed in July 2014, but the campaign itself was active in October 2013. According to reports, attackers used brute-force techniques to remotely access desktop servers and install the Backoff malware. Backoff is capable of extracting payment card data by scraping memory and exfiltrating data over HTTP. Backoff's command-and-control (CnC) servers are connected to those used to host Zeus, SpyEye, and Citadel—suggesting that Backoff may be connected to a broader series of attacks.

2 BrutPOS

The BrutPOS malware was first documented in July 2014. This botnet scans specified ranges of IP addresses for remote desktop servers. If a POS system is found, the attackers may deploy another variant that scans the memory of running processes to extract payment card information. BrutPOS exfiltrates data over file transfer protocol (FTP).

3 Soraya

The Soraya POS malware was disclosed in June 2014. It iterates through running processes and accesses memory to extract payment card data. Soraya also has form-grabbing capabilities and exfiltrates data over HTTP.

4 Nemanja

The details of the Nemanja were disclosed in May 2014 and the botnet is believed to have been active throughout 2013. The attackers compromised an array of POS machines worldwide running a variety of POS software. The attackers were reportedly directly engaged in the production of fake payment cards and money laundering using mobile POS solutions.

5 JackPOS

The JackPOS malware was reported in February 2014. According to accounts, it originally spread through drive-by download attacks. The malware, which appears to be related to the Alina malware, can scrape memory to acquire payment card data and exfiltrate it over HTTP. JackPOS is now widely available on underground forums and is used by an assortment of threat actors.

6 Decebal

The Decebal POS malware was first reported in January 2014. The malware enumerates running processes and extracts payment card information. That information is then exfiltrated over HTTP.

7 ChewBacca

The ChewBacca malware was first disclosed in December 2013. Using two regular expressions that match payment-card data formats, this malware enumerates running processes and accesses memory to extract information. This malware uses the Tor anonymity network to exfiltrate data.

8 BlackPOS

The BlackPOS malware, sold on underground forums by an individual believed to be "ree4," was first reported March 2013 and is now widely available. This malware, which has a variant also known as KAPTOXA, scrapes memory to obtain payment card data. This data is usually transferred to a local staging point and then exfiltrated using FTP. The malware is best known for its reported role in several highly publicized breaches.

9 Alina

The Alina POS malware, first disclosed in February 2013, is believed to be the brainchild of "dice," who also helped develop the Dexter POS malware (see below). This malware has been reportedly distributed via Citadel botnets. The Alina POS malware iterates through running processes (except those on a blacklist) and dumps the memory, looking for payment card data before exfiltrating it over HTTP. While this malware initially was used by a select few, it was then sold on underground forums.

10 vSkimmer

The vSkimmer malware was first disclosed in January 2013. It is available on a variety of underground forums is used by multiple threat actors. The malware iterates through running processes and accesses memory to extract payment card information. Then it exfiltrates that data over HTTP.

CONCLUSIONS AND RECOMMENDATIONS

More than six months—and countless high-profile data breaches—after our original report, the attacks haven't stopped. As our newest data shows, data breaches remain commonplace.

This continued shortcoming is especially alarming given that nearly all of the advanced malware used in these breaches are well-known to security researchers and vendors. And still, conventional tools are not stopping them.

FireEye is happy to see others taking steps to raise the awareness of these gaps as well. Recently, security testing company Delta Testing, who focuses on running tests based on to real-life deployment scenarios, published a report showing significant gaps in many well-known advanced security vendors. This report confirms FireEye's previous reports on the prevalence of advanced malware in enterprises today, as well as challenges traditional security vendors have with the evolving threat landscape.

As we said in the original report, organizations must consider a new approach to securing their IT assets. They need to move away from passive, poorly integrated defenses that provide a fragmented view of threats and cannot connect the dots in advanced attacks. They need a tightly integrated, nimble architecture that enables big-picture vigilance. Today's security organizations can't afford to passively wait for attacks. Instead, they should take a lean-forward approach that actively hunts for new and unseen threats.

We call this approach FireEye Adaptive Defense. ™

To find out how FireEye Adaptive Defense can help your company prevent, detect, analyze, and respond to today's advanced threats, visit fireeye.com.

For more information about FireEye Adaptive Defense,
visit our website: **www.fireeye.com**

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | **www.fireeye.com**