Invincea 1H 2015 Advanced Endpoint Threat Report

August 2015

Invincea 1H 2015 Advanced Endpoint Threat Report

Contents

Introduction…… 3
The billion dollar malvertising problem……..3
Just-in-Time Malware assembly……6
Weaponized Office documents as email attachments……8
The ongoing Fessleak ransomware and click-fraud campaign…...12
White House and Anthem breaches……15
Conclusion……...22
Appendix: Monthly advanced endpoint threat trends……24

Introduction

In the rapidly changing threat environment, security professionals need timely information on the latest threats and adversary techniques, as well as perspective on what is most significant over a broader population and time frame. This semiannual advanced endpoint threat report from Invincea documents the noteworthy threats Invincea observes, often weeks before other security firms due to Invincea's non-signature-based sensors deployed across our global user base.

With two million users running Invincea Advanced Endpoint Protection across a range of industries, organizational sizes, and countries, Invincea has a uniquely broad view into the latest malware and attack vectors. We used this perspective to identify and illustrate the key advanced endpoint threat trends, as well as broader industry events, during the first six months of 2015.

What makes these threats notable is that they succeeded in evading every other security control present in the enterprise – network sandbox, next-generation firewall, network IPS/IDS, Web URL filtering and proxy, email gateway, threat intelligence feed, anti-virus, and other security technologies. They are the threats on which enterprise security teams should focus the most attention.

This report highlights five trends and events that dominated the first half of the year:

- The billion dollar malvertising problem
- The rapid emergence of Just-in-Time Malware assembly
- The evolution of weaponized Office attachments
- The ongoing Fessleak ransomware and click-fraud campaign
- White House and Anthem breaches: Advanced adversaries, commonplace approaches

The billion dollar malvertising problem

Malvertising – the distribution of malicious web-based ads through third-party advertising platforms – involves sophisticated drive-by exploits, often leveraging zero-day vulnerabilities in browsers, Adobe Flash, and Java plug-ins to compromise end user devices. The malware delivered via malvertising in the first six months of 2015 was primarily ransomware, click-fraud bots, and banking Trojans like Zbot. June was by far the worst month on record for malvertising – likely due to the multiple Flash zero-day exploits that were integrated into exploit kits used to host fraudulent ads that month.

During the first half of 2015, Invincea observed approximately 2,100 malvertising attacks against customers, all of which were blocked by Invincea. These attacks represented 2.1 million malicious advertisements purchased by real-time ad bidding (RTB) malvertisers, which Invincea estimates caused $525 million of damage in repair and recovery expense, excluding the impact of any data breaches. At an industry average price of approximately $2.90 per thousand online ads, malicious actors were able to inflict more than half a billion dollars of damage for a mere $6,000 in advertising spend. On an annualized basis, the malvertising campaigns Invincea observed generate more than $1 billion in damage per year.

CryptoWall Malvertising Dropped on Zillow Users

In Figure 1 below, a visitor to Zillow.com encountered an ad window that delivered a Flash exploit. This exploit scripted an attack that assembled malware on the endpoint and named it MSIexec.exe, a typically whitelisted file name. This program called other native Windows utilities and eventually attempted to encrypt all files on the host. This attack makes extensive use of native Windows utilities, with the ultimate goal of rendering the system completely inoperable. Endpoints running Invincea, however, remained secure and unaffected. As in other cases of malvertising, Zillow.com was probably unaware of this threat posed by a third party.

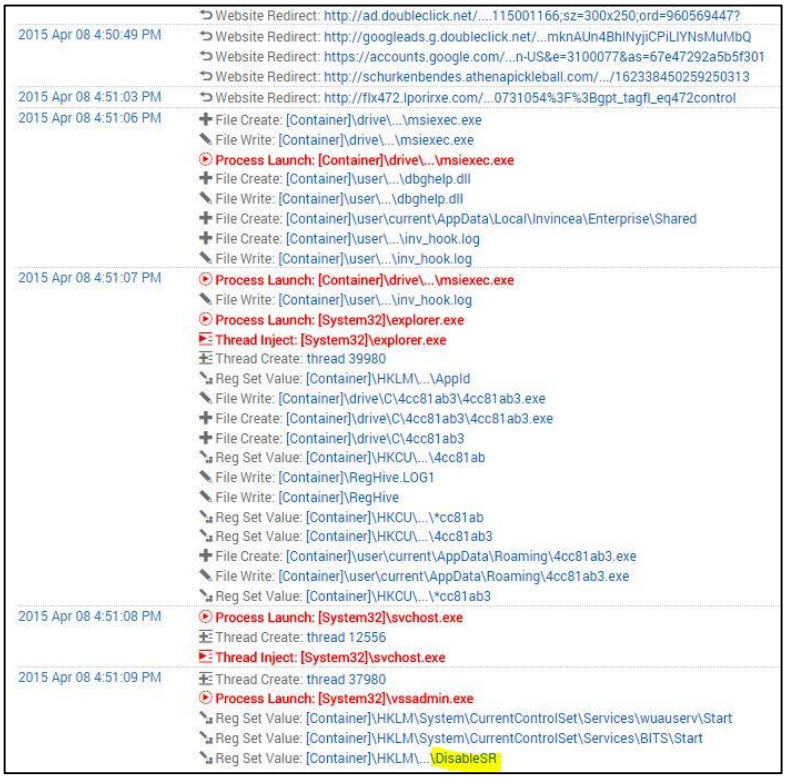
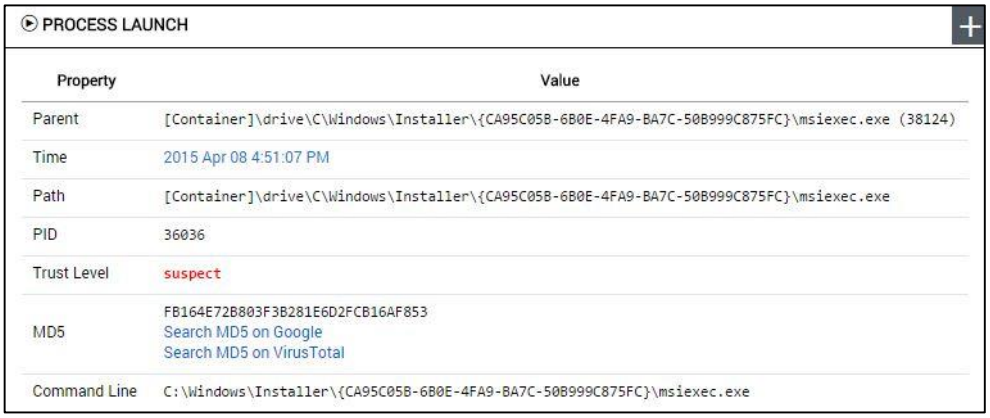


Figure 1: CryptoWall malvertising that used MSIexec and Svchost.exe

Figure 2 shows how the Flash overflow modified the system registry and launched the fake MSIexec installer. All attempted changes were isolated in the Invincea container and could not persist.

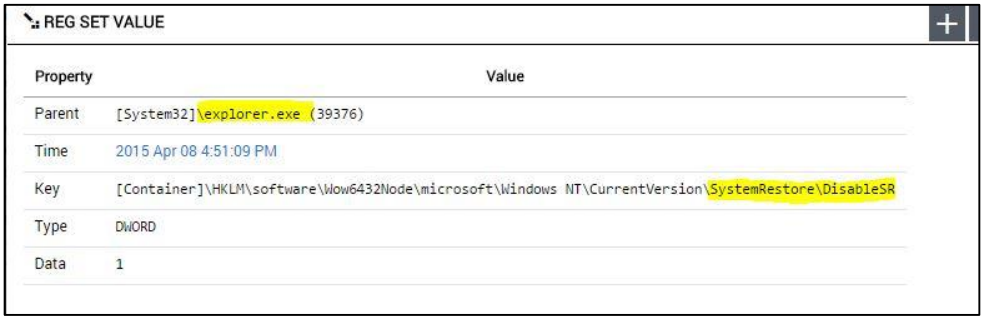


PROCESS LAUNCH

Property	Value
Parent	[Container]\drive\C\Windows\Installer\{CA95C05B-6B0E-4FA9-BA7C-50B999C875FC}\msiexec.exe (38124)
Time	2015 Apr 08 4:51:07 PM
Path	[Container]\drive\C\Windows\Installer\{CA95C05B-6B0E-4FA9-BA7C-50B999C875FC}\msiexec.exe
PID	36036
Trust Level	suspect
MD5	FB164E72B803F3B281E6D2FCB16AF853 Search MD5 on Google Search MD5 on VirusTotal
Command Line	C:\Windows\Installer\{CA95C05B-6B0E-4FA9-BA7C-50B999C875FC}\msiexec.exe

Figure 2: MSIexec called to install ransomware

Next, the malware disabled the System Restore capability in the system registry. Without the ability to automatically recover, the victim would be more likely to pay the ransom.



REG SET VALUE

Property	Value
Parent	[System32]\explorer.exe (39376)
Time	2015 Apr 08 4:51:09 PM
Key	[Container]\HKLM\software\Wow6432Node\microsoft\Windows NT\CurrentVersion\SystemRestore\DisableSR
Type	DWORD
Data	1

Figure 3: Explorer used to disable System Restore

The malware also accessed the Windows Shadow Copy utility, VSSAdmin.exe. The shadow copy is the last known good copy of the Windows core file system and registry settings, created and maintained automatically by Windows and commonly referred to as the “Last Good Copy.” By deleting the shadow backup copy of Windows, the victim would be more likely to pay the ransom.

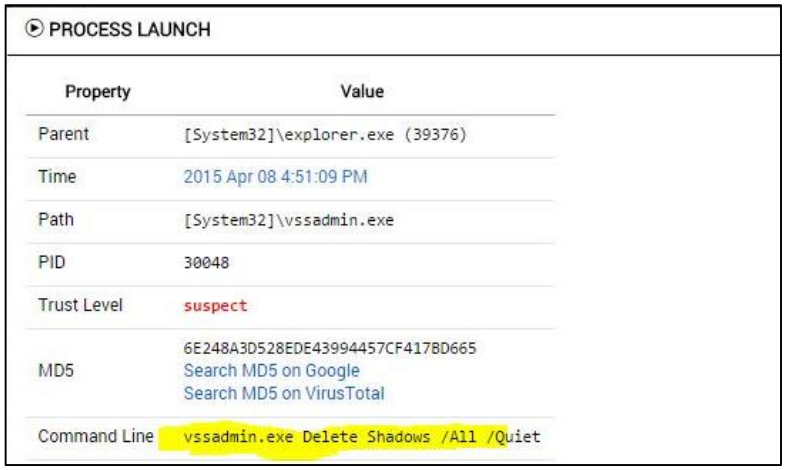


Figure 4: Explorer is used to access the VSSAdmin utility to wipe all shadow copies

This malware is programmed to wait for five minutes before encrypting the drive. It then accesses another Windows utility, this time using notepad.exe to display a message that the user's files are encrypted and to demand a ransom payment to decrypt the files. Again, Invincea isolated all malicious activity; the underlying system and data were secure and untouched.

Just-in-Time Malware assembly

A key trend in malware evolution during the first half of 2015 was the rapid emergence of just-in-time (JIT), on-host assembly of malware. This novel approach evades detection from network sandbox and many other security solutions. JIT malware is unlike traditional malware that is installed as an executable via drive-by download exploits, email attachments, or social engineering. Instead, JIT malware uses techniques borrowed from late-binding compilers to assemble a malware executable on the target endpoint itself in order to evade network sandbox analysis. In addition, the approach employs native Windows utilities from the target machine to assemble the payload, thus borrowing system software from the victim system in order to compromise it. This is useful in evading endpoint white-listing approaches that allow only approved programs to run.

Just-in-time malware assembly compromises systems while evading detection from network sandbox and traditional endpoint security solutions.

Figure 5 illustrates the lifecycle of on-host JIT malware assembly. Like most compromises, it begins with an application exploit, typically the browser or a plug-in such as Adobe Flash. Often some portion of the payload is downloaded with the exploit and retained in memory. Command shell or other scripting engines on host are used to begin to assemble the various code snippets together, employing crypto primitives such as XOR techniques. After this, the payload is launched. Depending on the sophistication of the attack, it can be dropped to disk as an executable and launched, or in some cases simply launched within memory. The use of powershell.exe, host scripting, and VBScript assembly, coupled with vulnerabilities in browsers, Office applications, and plug-ins such as Flash, are prime elements that enable this technique.

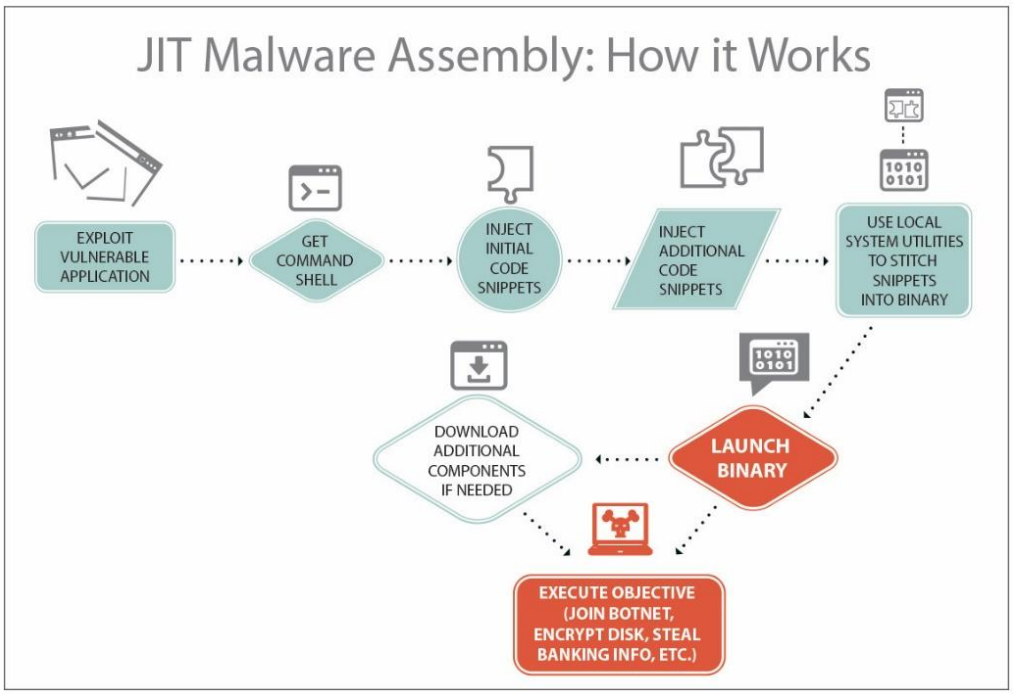


Figure 5: How JIT malware assembly works

Most network sandboxes, such as FireEye, look for executables in network traffic in order to copy or remove them and “detonate” them within a sandbox to determine their potential for harm. But this requires the identification of an actual executable in network traffic. With JIT malware assembly, a variety of approved system utilities and applications assemble the payload on the host in multiple stages. Threat actors

are now having great success in evading network sandbox, IDS, and traditional endpoint security solutions with this multi-stage delivery / JIT assembly approach.

Network solutions are largely blind to these attacks because there is no single payload entering from the outside that looks or acts malicious—only fragments of code that appear innocent, or to a network monitoring system, appear as blobs of bits. There are no PE headers in the code to indicate when to begin capture, nor an executable within the network payload that can be extracted and examined.

Standard endpoint threat detection solutions are also fooled because the run-time assembly of code takes advantage of standard Windows files and applications, most of which would be white-listed by process monitoring and application control security tools.

Network solutions are largely blind to these attacks because there is no single payload entering from the outside that looks or acts malicious—only fragments of code that appear innocent, or to a network monitoring system, appear as blobs of bits.

JIT malware assembly is an over-arching trend across multiple threat vectors and was observed coupled with many modern malware families over the period of study. Dridex, Dyreza, Pony, Zbot, and Zeus malware were often delivered via spear-phishing or malvertising, and sometimes combined with ransomware. Invincea observed these attempted infections use JIT assembly to bypass legacy enterprise controls; our global customer base relied on Invincea as the final layer of protection to stop the threats that evaded other layers.

Weaponized Office documents as email attachments

Weaponized Office documents (Word, Excel, and PowerPoint files) sent via email were one of the top threats in the first half of the year. Vulnerabilities in Microsoft Office applications were exploited by multiple criminal gangs via phishing emails to compromise endpoints, often to install Trojans that steal online banking credentials.

Dridex

Since the advent of the Sandworm family of malicious VBScript macro-enabled Office documents, Office attachments have become a primary method of delivering malicious binaries to endpoints. This threat continues to grow and morph into increasingly advanced threats that most traditional security solutions can neither prevent nor detect. The Visual Basic scripts are available on sharing sites such as Pastebin, allowing anyone who wants to craft his own weaponized documents to

engage in distribution of botnet, banking Trojan, or click-fraud malware. The delivery of weaponized Office documents and their malware payloads can now be considered "plug and play," as multiple threat actors have been observed using the same VB script to deliver their Trojan of choice.

These weaponized documents were most often seen delivered through phishing campaigns, posing as invoices, receipts, payroll errors, and other attractively named files. Most of these attachments automatically launched the embedded Visual Basic scripts, regardless of local settings to disable macros and scripting in Office attachments. Once launched, the Visual Basic script embedded in the document would invoke local scripting tools to "stitch" together the malware directly on the endpoint, using the code in the VB script combined with external code residing on a website, embedded in a gif or JPG image, or located within a seemingly benign JavaScript on an Internet host. Once combined, this JIT assembled malware was written directly onto the endpoint or run in memory, and then downloaded additional payloads from its command and control servers.

The Dridex banking Trojan quickly became the favorite of criminal gangs that used phishing documents to create their botnets. Following Dridex's success, other banking Trojans such as Pony and Dyreza soon began to spread using the same weaponized document VB code.

What began as simple scripting attacks involving Dridex soon evolved into multi-stage JIT assembly attacks, rendering perimeter detection by network sandboxing solutions such as FireEye ineffective.

In the first six months of 2015, Dridex and its accompanying weaponized documents employed notable evasion techniques to stay ahead of most security solutions. The payload hashes constantly changed, making anti-virus detection impossible. And what began as simple scripting attacks soon evolved into multi-stage JIT assembly attacks, rendering perimeter detection by network sandboxing solutions such as FireEye ineffective. The payloads also began using code-signed malware that bypassed whitelisting and application control solutions, and adversaries even moved their command and control hosts to the AWS cloud, thus evading proxy blacklisting.

Dridex Weaponized Word Document via Phishing

Figure 6 below shows the forensic information captured on a recent JIT malware attack that Invincea detected and prevented. Initially, a spear-phishing email containing a weaponized Word document is sent to a user. The Word document is empty except for fragments of Visual Basic Scripting and code that will launch

macros when the document is opened. Upon opening, Upatre, a notorious 1st stage installer Trojan, is assembled using VBScript (a native Windows scripting utility). Next, the exploit writes the script (GygywefgyFU.vbs) to a temp directory and then runs Wscript.exe, the Windows Scripting Host application, to execute the VBScript file. Sample VB scripts from Dridex can be found here. After this, the VBScript communicates with a command and control site (91.226.93.110:80) to download an encoded DLL file, which gets decoded by the original VBScript file. The final binary of 1233211.exe is then assembled from these components and written to disk. A different command and control site is notified, and the final Trojan is then launched. You can see more information on this Trojan at VirusTotal.

Figure 6: Wscript.exe used to deliver malicious payload from VB Script

Dyreza Weaponized Word Document via Phishing

This next instance also uses JIT malware assembly, initiated by a phishing attack with a weaponized Word document and embedded VBScript. This one opens a command shell on the host and immediately executes the Ping command, likely to validate it has permissions to execute commands within the System32 directory. It then calls the CHCP command, a Microsoft utility to validate the language character set of the host. This enables it to target specific language and keyboard sets.

After language validation, the malware calls Cscript.exe, a scripting utility similar to Wscript. Cscript echoes an output of the VBScript and batch files needed to assemble the routine to download malware from a command and control location. The malware needs to install this binary without alerting the end user that something is happening in the background. Thus powershell.exe is used.

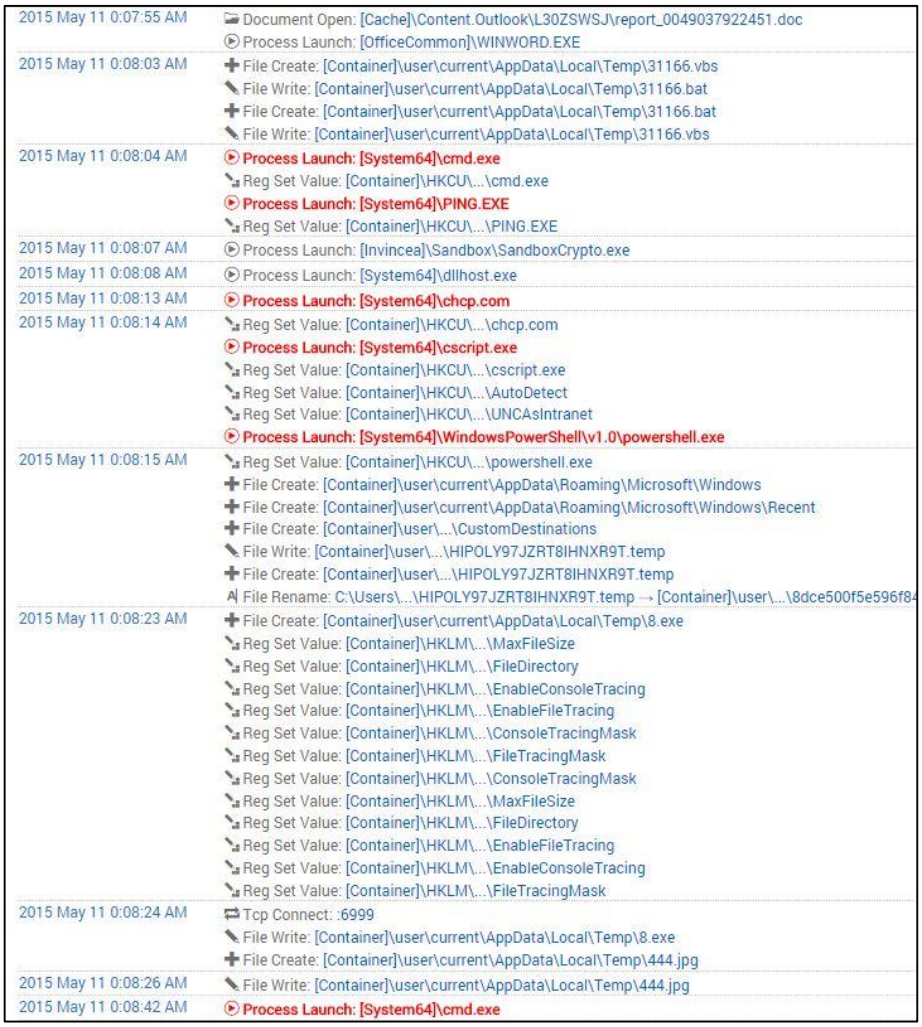


Figure 7: Cscript, CHCP and Powershell used to install Dyreza malware

The Powershell command shown in Figure 8 includes a switch to install the malware without alerting the end user. This bypass is noted by Microsoft here.

Figure 8: Powershell compiling the Dyreza binary from the temp directory, bypassing Execution Policy

Two additional payloads are delivered from the command and control site. The two executables according to the logs in Figure 7 are 8.exe and 444.jpg. This malware is summarized at VirusTotal.

Other weaponized documents delivered alternate payloads such as Zeus, Pony, Zbot, Dyreza and Facebook Hijacking Trojans. Each of these followed the example set by Dridex, often using the same delivery method, but swapping out the primary malware for its own.

The ongoing Fessleak ransomware and click-fraud campaign

Fessleak is the name given by Invincea to a notorious Russian threat actor who began abusing Real-Time Ad Bidding platforms in late 2014, to deliver click-fraud bots and ransomware via malvertising. Using the email alias fessleak@qip.ru, Fessleak had registered dozens of “burner” domains to host temporary exploit kits. Once Fessleak won an advertising bid auction, he would display zero-day Flash exploits instead of actual ads, and use his burner domains to host secondary exploits such as the Bedep click-fraud bot or his ransomware exploit. After Fessleak compromised thousands of victims via online ads, he would delete his crimeware tools and move onto the next registered domain.

Fessleak also used JIT malware assembly, coupled with a Flash zero-day command shell, to stitch the malware together directly on the endpoint. A full analysis of Fessleak is provided here.

Throughout the period under study, Fessleak continued to incorporate additional Flash zero-day exploits into his ransomware and click-fraud toolkits. Once evicted from one RTB platform, he would set up shop on another ad platform, continuing his malvertising campaign. Fessleak primarily targeted US broadband users for click-fraud infection. During the first half of 2015, Fessleak accounted for more malvertising exploits than any other threat actor observed across Invincea's 2 million users.

During the first half of 2015, Fessleak accounted for more malvertising exploits than any other threat actor observed across Invincea's 2 million users.

The combination of tactics used by Fessleak – including (1) use of malvertising on popular websites, (2) use of JIT assembly of malware, (3) use of 0-day Flash exploits from exploit kits, and (4) use of burner domains to foil domain sink-holing – rendered Fessleak unobservable by almost all security controls other than Invincea.

Malvertising Exploit Kit on eBay UK Delivers Backdoor Trojan

Fessleak may have been the first malvertiser to use the JIT tactics of a scripting attack coupled with a Flash overflow exploit to compile a binary on his victims' systems. Similar attacks by Fessleak and others are still taking place around the world, and even high-profile websites such as ebay.co.uk are susceptible to malvertising delivery via third-party ad networks. It is important to note that the websites on which malvertising appears, such as eBay, are largely unaware that their sites are being used by malicious advertisers to drop malware on their visitors, and most have no control over this, because attackers abuse the third-party advertising networks and manipulate Real Time Ad Bidding (RTB) to deliver exploits through ad windows.

In the logs in Figure 9, a victim visited eBay's UK site and was hit with a malvertising attack. The attack was delivered via a Flash advertising window, which spawned a CMD shell. This shell used an echo command to effectively write out the malware, coupling the echo commands to fill in gaps in a separately hosted JavaScript, shown below as wtm.js. Finally, Wscript was called to complete the binary compilation and launch the resulting Trojan backdoor. This JIT attack has three components: the Flash overflow, the hosted JavaScript, and the Windows scripting.

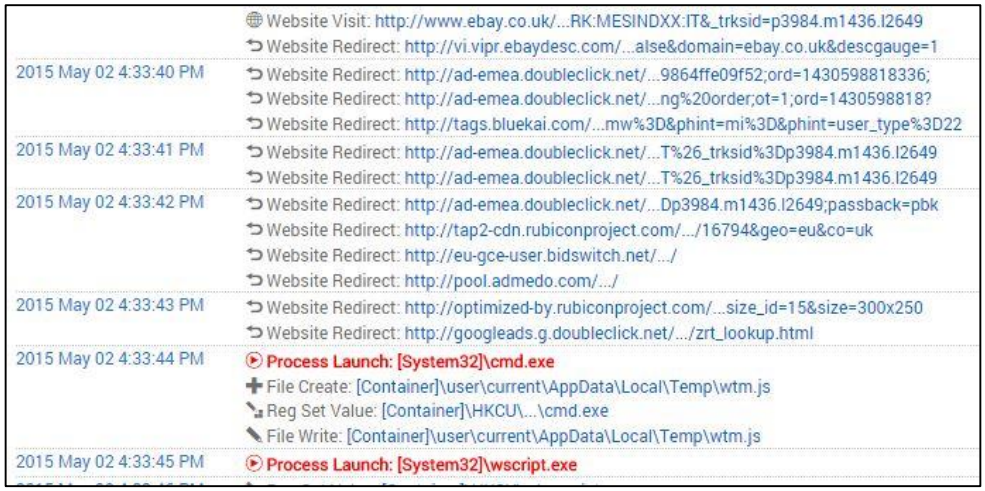


Figure 9: CMD scripting via echo commands and wscripting to install Trojans

The CMD shell and echo commands are detailed in Figure 10.

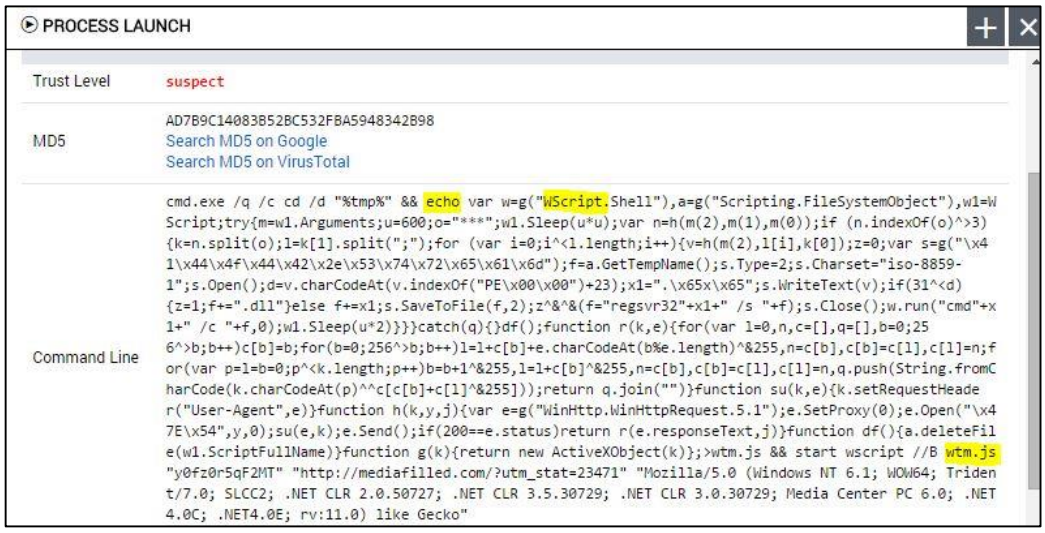


Figure 10: Echo commands from the Flash overflow which calls on a separately hosted Java Script to compile malware

And finally, a screenshot of the Wscript commands:

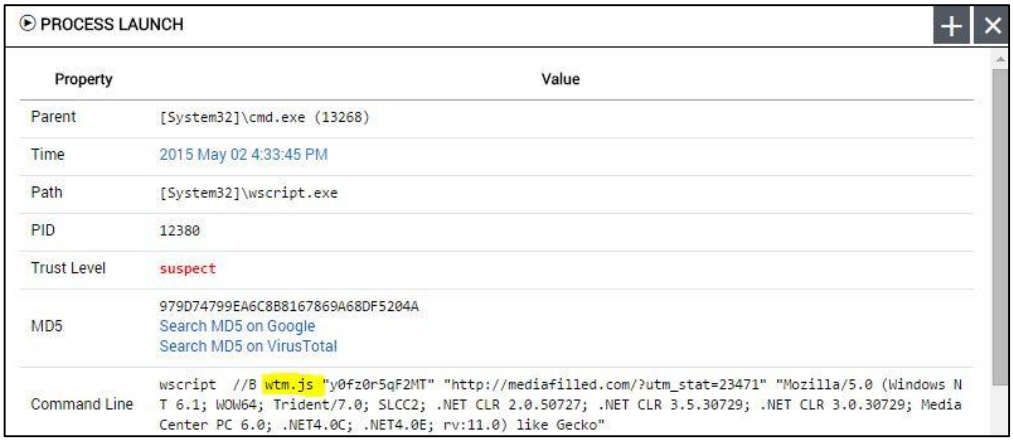


Figure 11: The Wscript commands to activate the external java script.

Most of these attacks create malware whose hashes have never been seen by any anti-virus vendor and are rarely detectable by AV during the first days/weeks of an attack. However, a similar malvertising attack occurring on ViewMixed.com delivered similar malware that is summarized at VirusTotal.

White House and Anthem breaches: Advanced adversaries, commonplace approaches

In two recent high-profile Advanced Persistent Threat (APT) campaigns, a similar attack vector was used to lure users into clicking on malicious content that enabled adversaries to gain a crucial beach-head on the targeted networks. The recent breaches of Anthem and the White House employed the same attack method – an email sent to users with a video or software update that, when opened, installed backdoors onto the endpoints for intruders to enter the network unnoticed. Such spear-phishing success demonstrates that common attack techniques work against even highly trained users in sophisticated organizations.

Invincea's analysis shows these attacks were conventional in approach even if sent by advanced threat actors – a common pattern in targeted attacks. Adversaries do not burn zero-day exploits when a simpler approach – spear-phishing with malicious attachments using known exploits – is just as effective. Published reports indicate the Chinese APT group Deep Panda targeted Anthem, while Russian actors reportedly targeted the White House. However, Invincea analysis shows that not only were the attack vectors nearly identical, but the malware used were also similar (although customized to avoid detection by traditional security tools). In the case of Anthem, a spoofed Citrix software installer helped trick a user into loading the malware. White House personnel were fooled by an "Office Monkeys" video that was likely shared among staff, making it socially viral as well as infectiously viral.

Anthem / Deep Panda Attack Analysis

Anthem, the nation's second-largest healthcare insurer, announced a major breach of its network in February 2015. Researchers were quick to share the indicators of compromise throughout the security community. The most comprehensive description of the attack was published by ThreatConnect, which attributed the attack to Deep Panda, a named Chinese APT group.

In ThreatConnect's write-up were two key Indicators of Compromise (IOCs): The original infector binary's hash and a domain of we11point[.]com. (Note the substitution of 1's for l's in wellpoint.com). Wellpoint Health Networks, acquired by Anthem in 2004, initially kept its wellpoint.com domain and brand, and only adopted the Anthem name in December 2014. However, the wellpoint.com domain was still familiar to Anthem personnel. The domain we11point[.]com appears to have been created to spear-phish Anthem's IT staff into installing what they believed were updates to Citrix. This threat arrived via email with a malicious link, an attack vector that deceives users into giving the adversary a presence on their network. The traditional enterprise defense for this attack vector is an email gateway solution that requires constant signature updating. If/when that fails to keep out threats, employees are relied on to determine what is potentially malicious, with significant negative consequences when the wrong decision is made.

Using an MD5 hash reported by ThreatConnect, Invincea obtained the malicious binary from public sources and ran it within the secure virtual container of Invincea Advanced Endpoint Protection, to safely observe how it behaved.

Upon executing, the malware displays a fake Citrix product installer – which is actually a video embedded in the malware – to trick the user into believing that a real Citrix update is running.

The malware is indeed installing files, but not what the user believes. Instead, several malicious executables are installed and executed. Next, the malware opens a connection to the we11point[.]com domain. Although we11point[.]com was still active as of this writing, it is not serving the original content that Anthem employees would have seen during the attack. Meanwhile, in the background, the malware is busy attempting to probe the network, install Trojans, and open access ports. Figure 12 displays an excerpt of the detailed forensic information gathered by Invincea on this event.

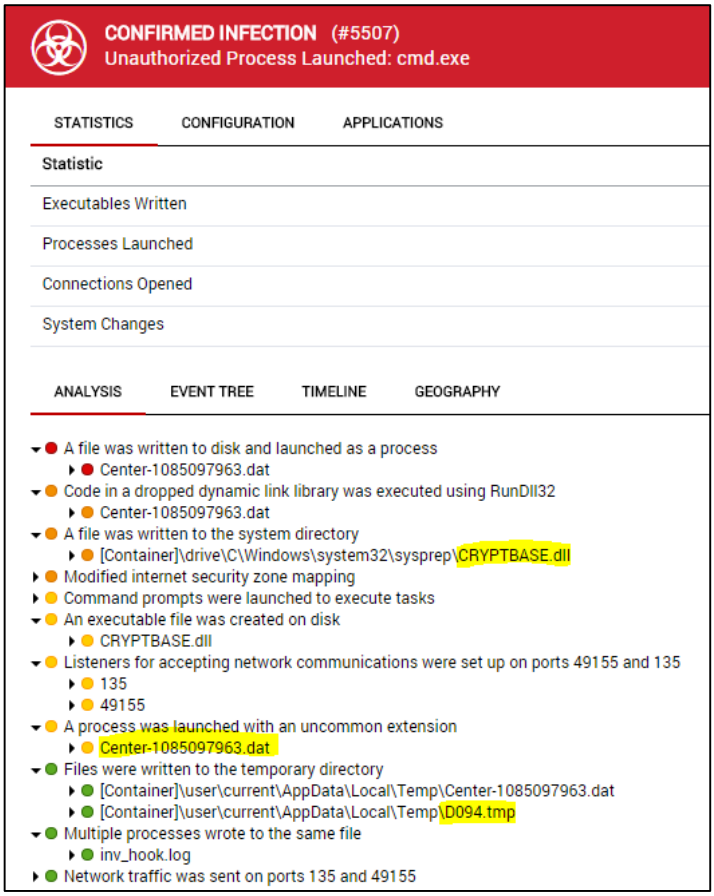


Figure 12: Invincea forensic summary of Anthem infection

After this, a program called D094.tmp was created and then deleted by the malware in a \Temp directory, and the network was probed to look for interconnected hosts. The D094.tmp file is the actual malware installer. A command prompt is called next, with the command line arguments instructing the system to execute the .DAT file, which is simply the fake product installation video mentioned earlier. Lastly, the malware runs another command shell to erase the original TMP file, in order to make file capture and analysis difficult for security analysts and researchers.

Cynomix Analysis of Anthem / Deep Panda Binary

If the targeted users had been protected by Invincea Advanced Endpoint Protection, the initial infector file called via email link would have been automatically analyzed by Invincea's Cynomix cloud-based analysis service. Cynomix is an advanced technology that performs static code analysis to determine the maliciousness and capabilities of unknown programs. Backed by four years of DARPA-funded development, Cynomix uses patent-pending cyber genome analysis technology to identify the similarity of a program's unique genetic markers to those in known

malware families. It uses machine learning and crowdsourced analysis to identify unknown malware.

As noted, many of the binaries used in the Anthem attack point toward the Deep Panda threat actor. Cynomix analysis indicates the original binary used against Anthem is likely an off-the-shelf Trojan, slightly customized. Figure 13 (a Cynomix screenshot) shows the initial infector is very similar to several known backdoor Trojans, including a second variant referenced in the ThreatConnect report, detailed at VirusTotal here. Notably, this second variant was also used to spear-phish defense contractor VAE, as per Krebs on Security. These two related variants are highlighted below.

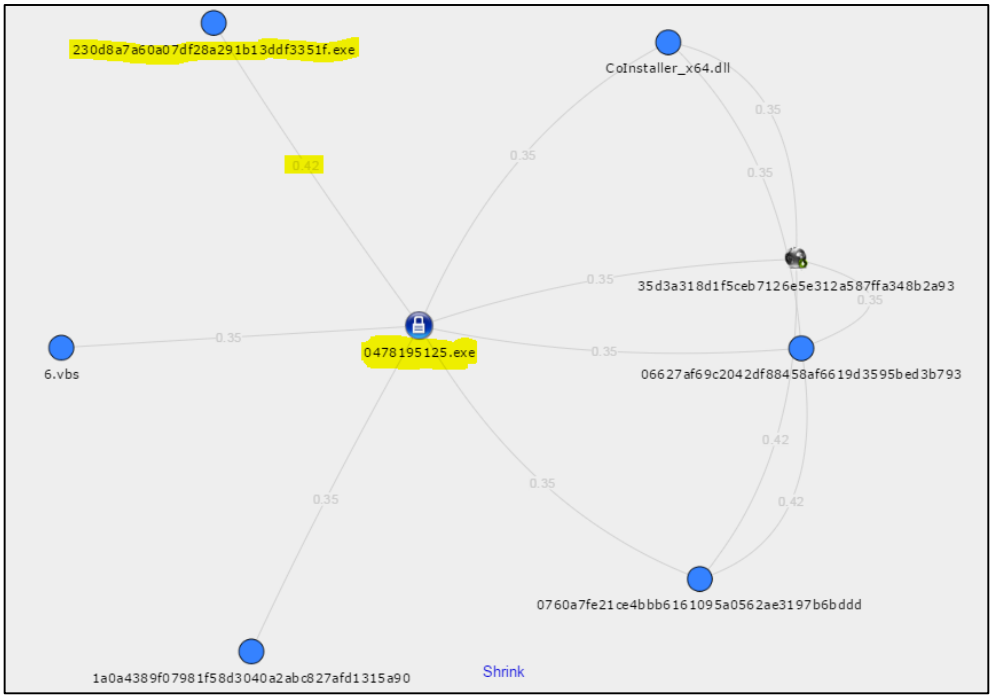


Figure 13: Anthem binary clusters with known Trojans; is most similar to Deep Panda binary used in VAE attack

Cynomix also identifies the functional capabilities possessed by binaries, allowing an analyst to determine what the unknown software can do, as well as how similar it is to other software. Figure 14 displays the capabilities of the Anthem binary and its similarities to other malware variants, with the closest relationship being the highlighted binary used in the VAE spear-phish attack. The Anthem binary has system and console access, keylogging, and screenshot capture capabilities.

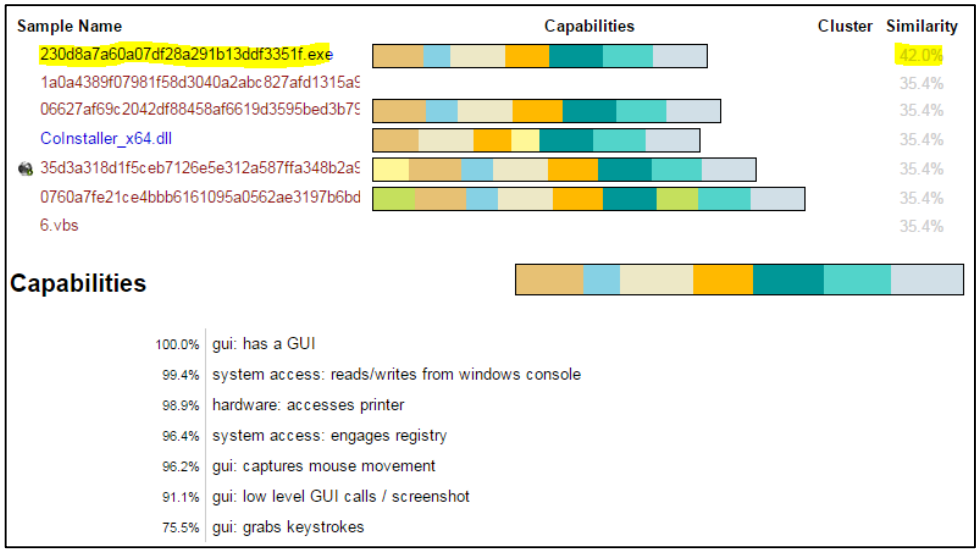


Figure 14: Functional capabilities & similarities to known malware documented by Cynomix

White House / CozyDuke Attack Analysis

A very similar attack reportedly targeted the White House, breaching unclassified networks. Instead of being prompted to run a spoofed Citrix installer, victims received a humorous video of monkeys running a business. The video not only went socially viral among the White House staff, but also became infectiously viral among their computers. This Threatpost article summarizes the story, including reports that the same CozyDuke threat actor also targeted the State Department and NOAA. As with the Anthem breach, reported research began with hashes of the malware. F-Secure provided a comprehensive list of hashes in its original published report. And just like with the Anthem/Deep Panda breach, this initial infection is reported to have started via a spear-phishing email attachment.

From the F-Secure report:

> *We have observed CozyDuke being spread via email, which usually contains a link to a compromised website hosting a ZIP file (although in at least one case, the file was hosted on Dropbox). These files contain an executable that, upon execution, will write to disk and execute CozyDuke, while… presenting the user with a decoy to divert attention. The decoy is usually an uninteresting PDF, but we have also observed a Flash video of monkeys as the decoy.*

Invincea began by analyzing each of the reported binaries in Cynomix. As with many lists of hashes, it was difficult to determine which was the binary used on

"Patient Zero" – the initial file used in the spear-phish. The answer to this puzzle came in a report by Securelist, which includes the following:

> *The actor often spear-phishes targets with e-mails containing a link to a hacked website. Sometimes it is a high profile, legitimate site such as "diplomacy.pl", hosting a ZIP archive. The ZIP archive contains a RAR SFX which installs the malware and shows an empty PDF decoy.*

As with the Anthem infector, we ran the CozyDuke malware on a system running Invincea Advanced Endpoint Protection, to simulate a user being spear-phished. The malware started by playing a video showing chimpanzees running a corporation and tormenting their human employee. Figure 15 shows a screenshot of this binary's behavior, including the malicious programs that run. Unlike with Anthem / Deep Panda, this binary fails to make any external connections, perhaps because its command and control infrastructure is no longer online. Regardless, a machine protected by Invincea will contain and detect this attack in real-time to prevent compromise, while reporting detailed forensics.

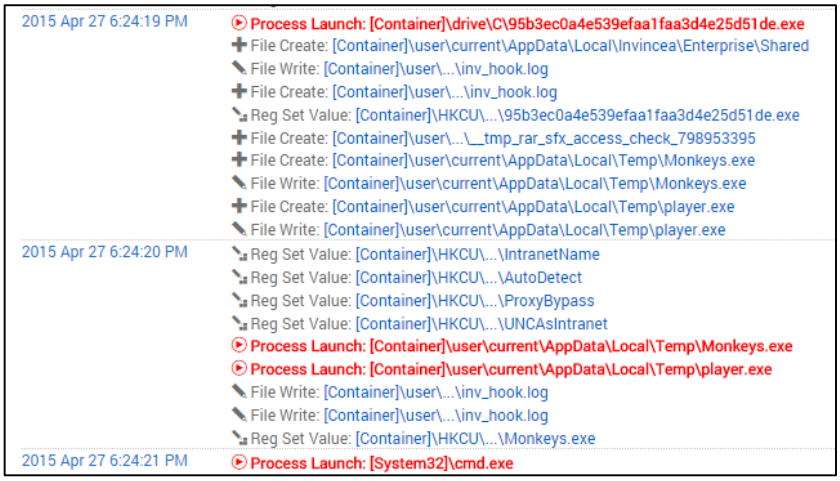


Figure 15: Detailed timeline of attempted system changes performed by CozyDuke malware

Cynomix Analysis of White House / CozyDuke Binary

The Cynomix analysis of the CozyDuke binaries produced some surprising results, contrasting with comments by Kaspersky and others that the perpetrator is likely a Russian APT threat actor. As Figure 16 shows, the Trojan used to penetrate the White House is very similar to several off-the-shelf Trojans, which according to file names, are likely used to phish or fool users into installing the binaries. Names like GTA San Andreas (a video game), Opera (the browser), and FixPlayer indicate that these Trojans had been used to socially engineer victims into installing the malware.

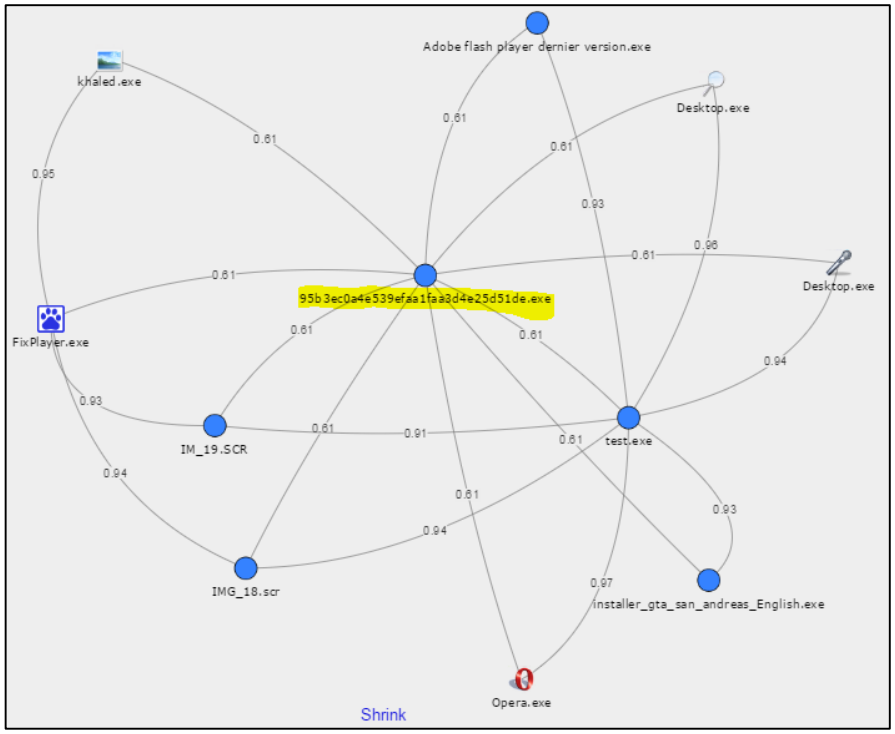


Figure 16: Trojan used in White House attack highlighted; note similarities to known Trojans

Figure 17 shows the Trojan's similarities to known malware and its functional capabilities, such as registry modification, screenshot access, and console access.

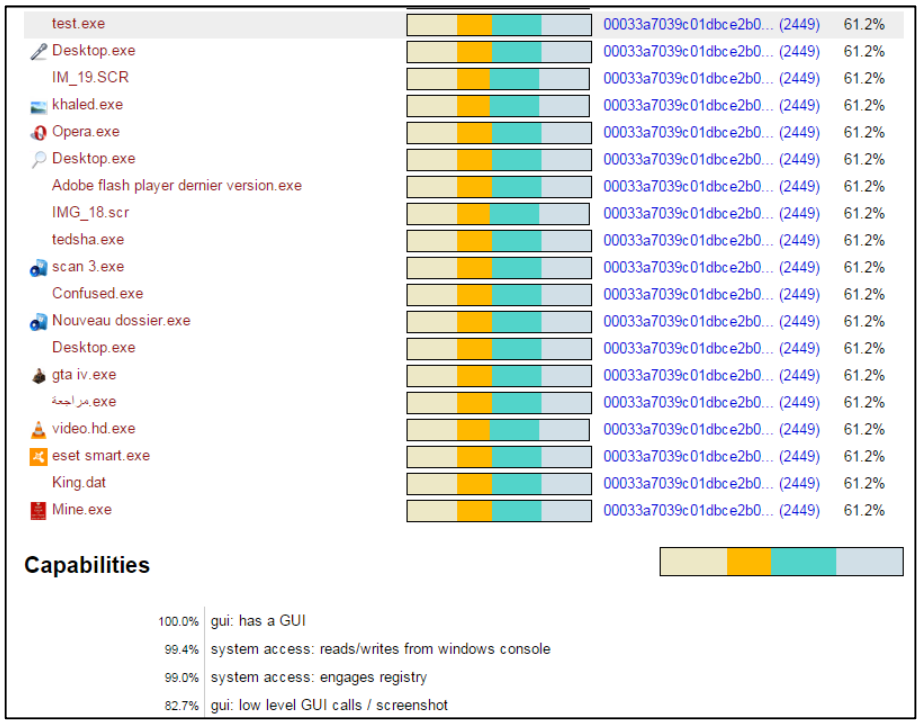


Figure 17: White House monkey video Trojan capabilities and similarity to known malware

What's most notable is that rather than create a purpose-built Trojan, the CozyDuke threat actor used an off-the-shelf piece of malware to perform the initial penetration into the White House network. The F-Secure report also detailed additional binaries used in the attack, many of which we analyzed in Cynomix. Most of these cluster well together, indicating that the binaries are similar to each other – and perhaps were even compiled by the same malware author, using the same tools, although this is not certain.

Deep Panda / CozyDuke Attack Conclusions

These attacks against Anthem and the White House were remarkably similar, raising questions about the presumed attribution to entirely different threat actors. Did a Chinese APT group attack Anthem and an unrelated Russian adversary attack the White House, using similar and largely off-the-shelf malware?

One unmistakable conclusion is that each attack gained initial access to its targets by exploiting an un-patchable weakness: the user. In each case, a spear-phish attack succeeded in gaining a foothold on the network, even though the targeted users were very security-aware. Each organization employed multiple layers of defense – including anti-virus, threat intelligence feeds, mandated employee security awareness training, and more. Yet all of these layers failed to prevent the breaches. The attack against Anthem brazenly targeted their cybersecurity personnel. White House employees had also received comprehensive security training, in an effort to prevent exactly this outcome – but to no avail.

These same adversarial tactics are being employed across numerous other US federal agencies and large commercial enterprises.

Conclusion

The threats documented here are among the most significant ones affecting businesses and government agencies today. Every security team should consider the following as they plan their 2015/2016 priorities:

- **Threats such as malvertising and weaponized Office attachments via spear-phishing are frequently evading all other security controls.** This report documents numerous attacks that sidestepped network sandbox, next-gen firewall, network IDS/IPS, Web URL filtering and proxy, and other security technologies. Invincea's secure virtual container served as the ultimate line of defense against just-in-time malware assembly, malvertising, spear-phishing, and other attacks.

- **These threats have demonstrated the ability to breach even Fortune 500 companies and government agencies.**
  Relying on "popular" security controls is no formula for success. When slightly modified off-the-shelf malware and a modicum of social engineering can breach Anthem and the White House, information security teams must re-evaluate their current approaches.
- **Security awareness training plays a role, but is far from sufficient to prevent breaches.**
  The failure of training initiatives to prevent these breaches is not new or surprising. Relying on users to make the right decision about every click is a failing strategy. Teaching users about online risks is useful, but relying on them to make the right decision 100% of the time is unrealistic. In addition, threats like malvertising – in which the user gets compromised while doing nothing wrong – render training less relevant.
- **The path forward must combine prevention with detection.**
  With the inability of anti-virus and other blocking technologies to stop threats, many security professionals shifted focus to rapid detection and response, based on a misguided view that "we can't stop the adversary." But detection-only solutions such as network sandboxes, IDS, and on-host IOC/signature sensors have failed to secure the enterprise, as adversaries attack users off-network, employ "burner" domains, and relentlessly morph their attacks. Even worse, these products provide a false sense of security.

With the emergence of next-generation threat protection solutions like Invincea, which is proven to block 0-day attacks with high effectiveness, the industry is regaining a balanced perspective on prevention and detection. Security leaders realize that every attack stopped is one fewer to detect and respond to. Every dollar spent on prevention is worth many times that much on detection and response. With the release of Invincea Advanced Endpoint Protection 5, organizations no longer have to choose between prevention and detection. Invincea combines the best prevention technology in the industry with a lightweight sensor and cloud-based machine learning, to detect pre-existing compromises and stop inbound threats.

The threats observed in the first half of 2015 represent a formidable challenge to information security teams. However, forward-looking organizations are finding ways to successfully navigate these waters, using Invincea for integrated threat prevention, detection, and response. While an APT attack is by definition persistent, such an adversary attacking Invincea-protected endpoints would have to find a new approach, since the enterprise's most vulnerable attack surface – the end user – is now safeguarded.

Appendix: Monthly advanced endpoint threat trends

Invincea live-tweets analysis of notable incidents that we detect and block in the wild. These are collected into monthly trend reports, which contain dozens of individual examples, including excerpted logs from advanced attacks.

[January 2015]
[February 2015]
[March 2015]
[April 2015]
[May 2015]
[June 2015]

About Invincea

Invincea is the leader in advanced endpoint threat protection, protecting more than 25,000 customers and 2 million active users.

The company provides the most comprehensive solution to contain, identify, and control the advanced attacks that evade legacy security controls. Invincea protects enterprises against targeted threats, including spear-phishing and Web drive-by attacks that exploit Java, Flash, and other applications. Combining the visibility and control of an endpoint solution with the intelligence of cloud analysis, Invincea offers the only market-deployed solution that defends against 0-day exploits, file-less malware, and previously unknown malware.

3975 University Drive, Suite 330, Fairfax, VA 22030 USA | Tel: 1-855-511-5967
info@invincea.com | www.invincea.com