The Modern Malware Review

Analysis of New and Evasive Malware in Live Enterprise Networks | 1st Edition, March 2013

paloalto NETWORKS

the network security company™

TABLE OF CONTENTS

BACKGROUND AND GOALS

The Modern Malware Review presents an analysis of 3 months of malware data derived from more than 1,000 live customer networks using WildFire™ (Palo Alto Networks™ feature for detecting and blocking new and unknown malware). The review focuses on malware samples that were initially undetected by industry-leading antivirus products.

A FOCUS ON ACTIONABLE RESEARCH

The goal of focusing on unknown or undetected malware is not to point out deficiency in traditional antivirus solutions—but rather to better understand the problems, and hopefully identify practices that can help. As such, the report provides analysis of the malware, but also includes recommendations based on the findings. Some of these recommendations are common sense, and we don't propose they are a panacea for modern malware and APTs. The goal is simply to share information that can help security teams be more proactive in their fight against modern malware and advanced threats.

SEPARATING THE KNOWN-UNKNOWNS FROM THE UNKNOWN-UNKNOWNS

Part of the problem when talking about advanced malware is agreeing what we really mean by modern malware. There is an incredible amount of malware diversity even when we focus on new and unknown malware. There are highly sophisticated, highly targeted sources of custom malware and APTs (e.g. APT1, Stuxnet, and Flame). But there are also legions of more traditional malware operations that generate malware at scale that are also able to get by traditional defenses (e.g. Zeus, Zero Access, Kelihos). Both of these categories present security risks that need to be managed, but obviously vary considerably in volume and the risk posed to the enterprise.

The latter, more common type of malware stands to potentially overwhelm security teams if each new variant of known malware requires a manual response from the security team. If too much "normal" malware goes undetected, then security teams will obviously have a very difficult time finding the truly targeted and unique threats in their networks. As a result we believe that it's crucial for enterprises to reduce the overall volume of infections from variants of known malware, so that security teams have the time to focus on the most serious and targeted threats.

One of the key values of being able to analyze real-world malware at a large scale is the ability to distinguish between common and repeated threats and those that are unique. As such, in the report we take a look both at the large-scale trends, but also at some of the samples that quite literally were exceptional. We hope the results of this analysis will help security managers to not only reduce the impact of the "known-unknowns", but also to reveal the presence of the "unknown-unknowns" as well.

ABOUT THE DATA AND THE METHODOLOGY

Malware samples were collected in live enterprise networks as part of the WildFire functionality for controlling modern malware. As part of our normal analysis we test malware samples collected by WildFire against fully updated antivirus products from 6 industry-leading enterprise antivirus vendors. This review focuses solely on all malware collected in a 3-month period that initially had no coverage from any of the tested vendors. This included more than 26,000 malware samples. Again, the intent is not to point out that some malware gets by traditional antivirus, but rather to provide actionable insight into the problem – what malware strategies are the most successful, why, and how can security teams do to respond.

Summary of Data Sources

- 3 months of WildFire data.
- 1,000+ live enterprise networks.
- Samples were tested against 6 fully-updated, industry-leading antivirus products.
- 26,000+ samples had no coverage at the time they were detected in live enterprise networks.

For the 26,000+ unknown/undetected samples, we used the application level visibility of the next-generation firewall in conjunction with the behavioral analysis of WildFire to provide as complete a view as possible of the malware lifecycle. This includes:

- **An application level analysis of the infecting malware session**: Samples were originally captured by the Palo Alto Networks firewall within customer deployments. Any infecting binaries were uploaded to Palo Alto Networks WildFire malware analysis cloud for further investigation. In most cases, binaries were accompanied by data concerning the infecting session such as a web-browsing session to provide insight into the infection strategy used by the attacker. It is important to note that these are only infection attempts observed by the firewall and does not mean that the infection was successful on the actual target.

- **The behavior of the malware on the host:** After the initial collection of the malware, all further analysis was performed in the WildFire cloud. This includes an active analysis of the malware in a virtualized host environment, allowing Palo Alto Networks to observe exactly how the sample behaves on a target and any techniques used by the malware.

- **An application level analysis of traffic generated by malware:** The vast majority of modern malware will make use of a network to steal data, orchestrate an ongoing attack against the network or download additional malicious payloads. For this reason, we closely analyzed the traffic generated by the malware itself in order to better understand the techniques used by malware to communicate.

ABOUT WILDFIRE

WildFire is an optional feature of Palo Alto Networks next-generation firewall that enables users to detect and block new and otherwise unknown malware. The solution leverages the firewall to look within network traffic for files that are unknown (neither known good, nor known bad). When an unknown file is detected, the file is copied and executed in Palo Alto Networks cloud-based environment where the file can be analyzed as malicious or benign based on the behavior of the malware. When a malicious file is detected, WildFire generates new protections based on the internal identifiers within the malware, which are delivered back to the firewall where enforcement occurs.

SUMMARY OF KEY FINDINGS

1. THE WEB IS THE FRONT LINE OF THE FIGHT AGAINST UNKNOWN MALWARE

- 90% of fully undetected malware was delivered via web-browsing.
- It took antivirus vendors 4 times as long to detect malware from web-based applications as opposed to email (20 days for web, 5 days for email).

2. FTP WAS OBSERVED TO BE EXCEPTIONALLY HIGH-RISK

- Samples from FTP were unique (94% of samples were seen only once).
- Samples from FTP were rarely gained coverage by AV (95% never gained coverage).
- Highly evasive and port independent—97% of FTP samples used only non-standard ports.

3. AN OPPORTUNITY TO TAKE ACTION – 70% OF MALWARE SHOWED INDICATORS IN THE PAYLOAD OR TRAFFIC

- 40% of unknown samples were related based on specific identifiers in the malware header and body.
  - A single indicator was linked to more than 1,200 unique SHA values.
- 30% of samples were observed to generate custom UDP or TCP traffic.
  - Custom or unknown traffic was the 3rd most common type of traffic generated by malware, trailing only web-browsing and DNS traffic.
- More than 30% of samples connected to new or unknown destinations on the Internet.
  - Unregistered or newly registered domains.
  - Newly registered DNS servers or dynamic DNS domains.

4. MALWARE SPENDS SIGNIFICANT EFFORT AVOIDING SECURITY

- 52% of observed malware behaviors focused on evading security or analysis, compared to only 15% focused on hacking and data theft.
- Attempting a long sleep to avoid analysis was the #1 most common malware behavior overall.

WEB TRAFFIC IS WHERE THE PROBLEMS ARE

It isn’t enough to simply know that there are threats that get by our traditional security. If we are going to actually improve in this area, then we need to learn what makes these more modern classes of malware different and how they actually work. In this section, we start with the basics and set out to get a better understanding of the characteristics of this malware and how it gets delivered.

Since the nascent days of the Internet, email has been the vector of choice for attackers delivering malware to a target, but that trend is rapidly changing. While email certainly continues to be a major source of malware, attackers are increasingly turning to real-time, web-enabled applications to deliver malware that is undetectable by traditional antivirus solutions. These real-time applications provide practical and technical advantages for an attacker, and the data shows that they are disproportionally successful at avoiding traditional antivirus as compared to email.

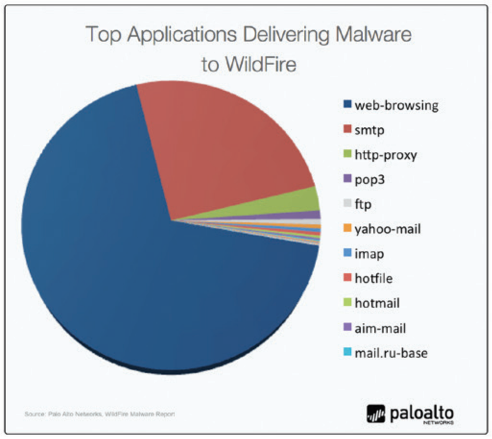
To better understand this phenomenon, we regularly test all malware samples captured by WildFire against fully updated antivirus products from 6 leading antivirus vendors. This provides a simple method for identifying malware samples that are undetectable by traditional AV, and thus pose particular risk to an enterprise. Over a 3-month period, WildFire analyzed 68,047 samples that were determined to be malware, and roughly 40% of those samples (26,363) were not detected by any of the tested antivirus products at the time the samples were captured in customer networks.

90% OF UNKNOWN MALWARE DELIVERED VIA WEB-BROWSING

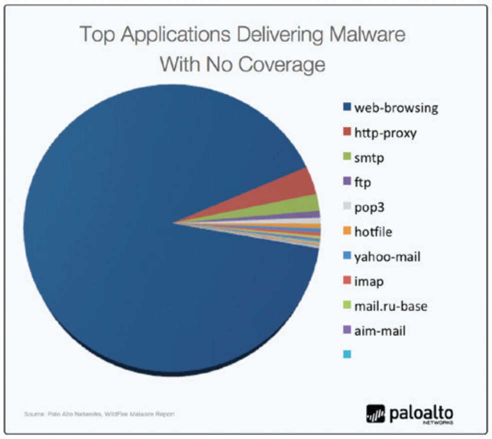
Given that the samples were captured by the firewall, we were able to identify the application that carried the malware. While web-browsing was found to be the leading source of malware both in terms of total malware* as well as undetected malware, the application mix was very different between the two groups. For example, SMTP accounted for 25% of the total malware, but only 2% of the fully undetected malware. Comparatively, web-browsing dominated both categories, accounting for 68% of total malware, but over 90% of undetected samples. This clearly shows that unknown malware is disproportionally more likely to be delivered from the web as opposed to email.

** Note:*
It is important to remember that all malware analyzed for this report was captured by customer firewalls, and may not represent all email-borne malware depending on where the firewall is deployed. As such, the data should be used to show which applications are relatively the most successful at delivering unknown malware, not which delivers the most total volume of malware.

All Malware Detected by WildFire	All Malware Detected by WildFire - No Coverage
68,047 Malware Samples	26,363 Malware Samples
68% Delivered via Web-Browsing	90% Delivered via Web-Browsing
25% Delivered via Email	2% Delivered via Email


Top Applications Delivering Malware to WildFire

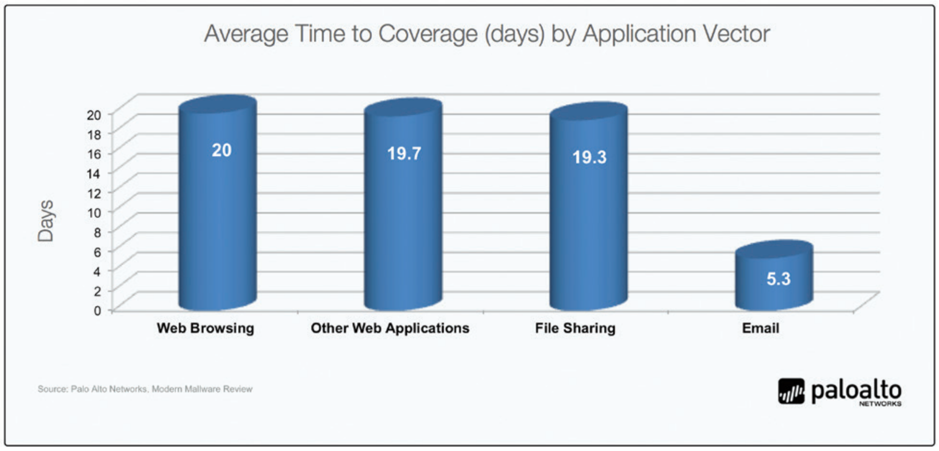
Source: Palo Alto Networks, WildFire Malware Report


Top Applications Delivering Malware With No Coverage

Source: Palo Alto Networks, WildFire Malware Report

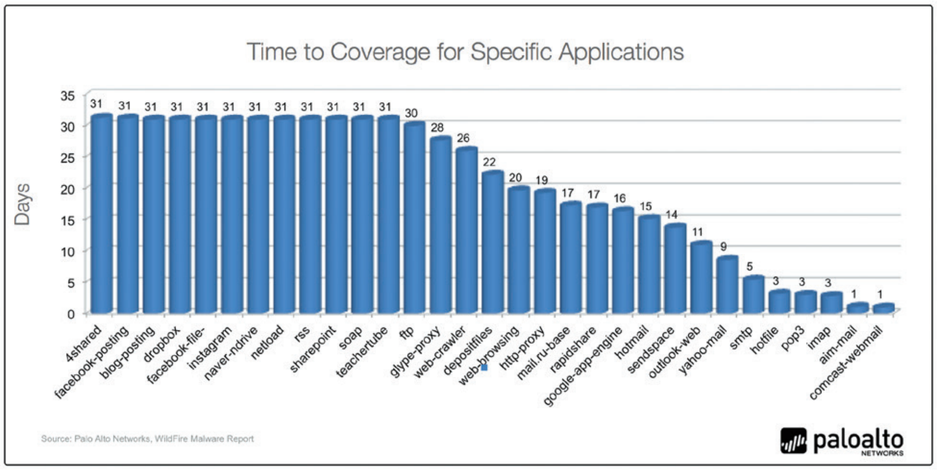
5 DAYS TO COVERAGE FOR EMAIL, 20 DAYS FOR EVERYTHING ELSE

To extend the analysis, we continually retest newly identified samples on a daily basis (for up to 30 days) to observe how industry coverage changes over time. This showed that not only are traditional AV solutions far less likely to detect malware outside of email, but also it takes far longer to get coverage. For unknown malware delivered by email, it took an average of 5 days for vendors to provide coverage compared to an average of 20 days for other applications, with many samples remaining undetected for the entire 31 day period.



Source: Palo Alto Networks, Modern Malware Review

Several applications delivered samples that remained undetected for 30 days or more, but had far fewer samples. Social media and file-sharing were common vectors in this category. The fact that these applications were used rarely by malware should not be confused with being low-risk. The more rare sources of malware were also more unique and often targeted in nature. The chart below shows a list of specific applications and their relative times to coverage by traditional antivirus. Applications with significantly high times-to-detection should be closely monitored by security teams. FTP had the ignominious distinction of being both a common source of unknown malware as well as one of the sources that rarely received coverage.



Source: Palo Alto Networks, WildFire Malware Report

CHALLENGES OF WEB-BASED MALWARE

There are a variety of reasons why web-based malware presents such a challenge for traditional antivirus products. First, web-browsing and other web-based applications are real-time by nature, unlike email where a malicious file can be analyzed at rest on a mail server. This has the effect of significantly shrinking the timescale in which detection and enforcement decisions must be made. However a potentially more significant factor is that web-based malware easily leverages server-side polymorphism, which simply means that the webserver that delivers the malware can automatically re-encode the malware payload to appear unique. This has the effect of generating vast amounts of unique malware on demand, which vastly reduces the likelihood that AV vendors will be able to capture the sample and create a signature. This is obviously very different from email-based malware, which are often sent out in bulk and are easily captured by antivirus vendors.

CONCLUSIONS AND RECOMMENDATIONS

In order to better address unknown malware, we first have to better understand where our traditional defenses are failing. The data shows that web-based applications are significantly more successful at both avoiding traditional antivirus and remaining unknown for extended periods of time. This means that organizations need to continue to expand their anti-malware strategies to include real-time network-based controls designed for these threats. These controls can come in a variety forms that are not limited to next-generation firewalls. In the coming sections, we will dig deeper into more specific indicators and techniques that can be put to use. However, at an architectural level, organizations should consider the following steps, if not already implemented.

- **Bring antimalware technologies into the network**: For many years, antimalware technologies lived on the desktop and network security lived in the network. The data shows that malware has found particular success by moving to a more real-time use of the network, and as such security teams should expect and be prepared to enforce at the network as well. This means that we will need to not only incorporate antimalware technologies in new places, but we must also do it at new speeds.

- **Expect unknowns, and add the ability to definitively identify malware:** Unknown malware is rapidly becoming normal and not the exception, and security must acknowledge this shift. The malware in this report was identified by actively executing unknown samples in order to see what they actually do. While this is not the only solution to the problem, the more important point is that teams need an automated way to determine if unknown files are malicious or benign that can be integrated into large networks.

- **Real-time detection and blocking whenever possible:** In many ways security has experienced a regression from a mindset focused on prevention to one based on detection. Detection is always the important first step, but prevention is key to a manageable security process. Malware is being generated at scale by malicious web-servers, with each variant being slightly unique. If each one of these variants requires a manual response, then security staff will remain behind the curve, and have little chance of catching the more truly targeted and sophisticated attacks. We will address some first steps and strategies in the coming sections.

- **Enforce User and Application-based Controls on Applications That Can Transfer Files:** Organizations should attempt to reduce their exposure and attack surface based on user and application controls in addition to improving the ability to detect and block unknown malware. For example, HTTP-proxies were a common source of malware. Organizations should ensure that only their corporate proxies are allowed and end-users are prevented from using their own web-proxies, which are often used to circumvent security policy. In the case of Facebook, teams may allow Facebook, but specifically limit the Facebook file transfer feature. Such basic steps can limit some of the exposure to both generic and targeted malware entering the network.

IDENTIFIERS IN UNKNOWN MALWARE

70% of unknown malware retained potentially actionable identifiers in either the malware payload or traffic.

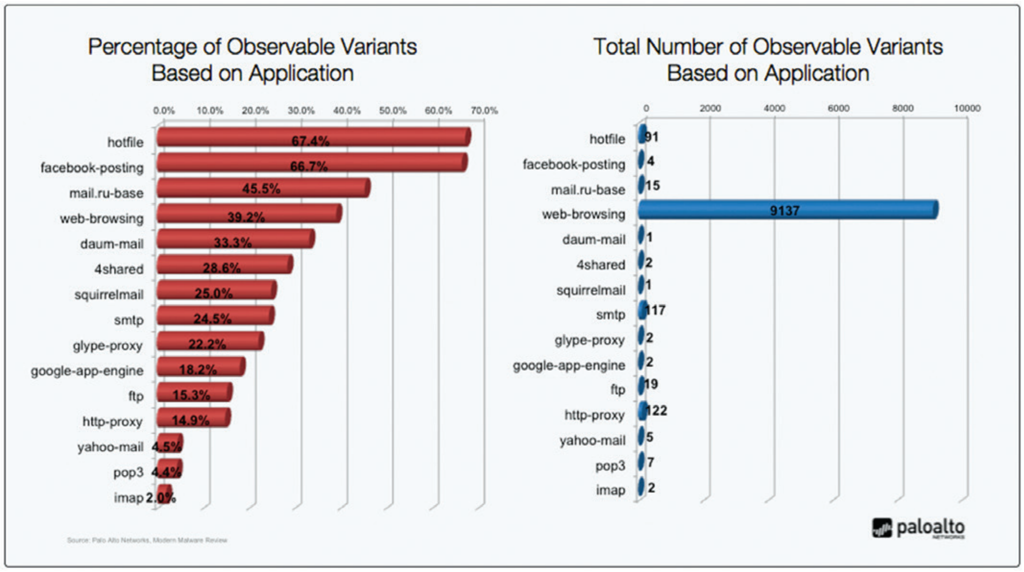
While malware has proven the ability to avoid traditional AV signatures, the news is not all bad. Our analysis combined an application level analysis of malware traffic (both inbound and outbound), the malware payload itself, as well as the malware behavior on a virtual host to find patterns that can be used to reduce an organization's exposure to unknown malware. Our analysis shows that of the more than 26,000 malware samples analyzed, 70% retained distinct identifiers or behaviors that can be useful for real-time control and blocking. While every indicator will not be appropriate for every network, the goal is simply to provide the research that security managers can adapt to their environments.

40% OF SAMPLES RETAINED ACTIONABLE IDENTIFIERS IN THE PAYLOAD

Even though when malware is modified in order to change the hash value of the file, the data shows that unique internal identifiers remained visible in more than 40% of the samples, which can be used to block malware downloads in real time. In short, a single signature was found to be able to protect against multiple variants of undetected malware each with unique sha256 values. This trend was consistent across web-browsing and other web-based applications that pose the greatest challenge to traditional antivirus products.

The identifiers were specifically visible in the header and body of the infecting file. This is significant because many network-based antimalware solutions will identify malware based on a hash value or URI, which would likely be ineffective in these cases. While blocking 40% of unknown malware does not solve the problem, it is encouraging to see techniques that can potentially reduce the volume of unknown malware, especially from web-based sources.

- 26,363 total unique malware samples (SHA256).
- 1,575 unique identifiers were observed in more than 1 piece of malware.
- These identifiers were observed in 10,616 unique malware samples.
- 40% of total unique malware had the potential to be blocked.



Percentage of Observable Variants Based on Application

Total Number of Observable Variants Based on Application

Source: Palo Alto Networks, Modern Malware Review

30% OF SAMPLES GENERATED CUSTOM OR UNKNOWN TRAFFIC

As malware has evolved, it has grown more and more dependent on the ability to infect, persist and manage itself over a network. In this regard, an understanding of how malware communicates is just as important as understanding the behaviors of the malware on the host. By combining information captured at the enterprise firewall in conjunction with traffic analyzed in the WildFire virtual environment, we were able to establish a very complete and unique view into malware traffic. Again, the analysis was focused on the more than 26,000 samples that were initially undetected by antivirus, with a particular focus on evasive techniques observed in the malware traffic as well as distinguishing characteristics in the traffic that can provide an indicator of a threat or compromise.

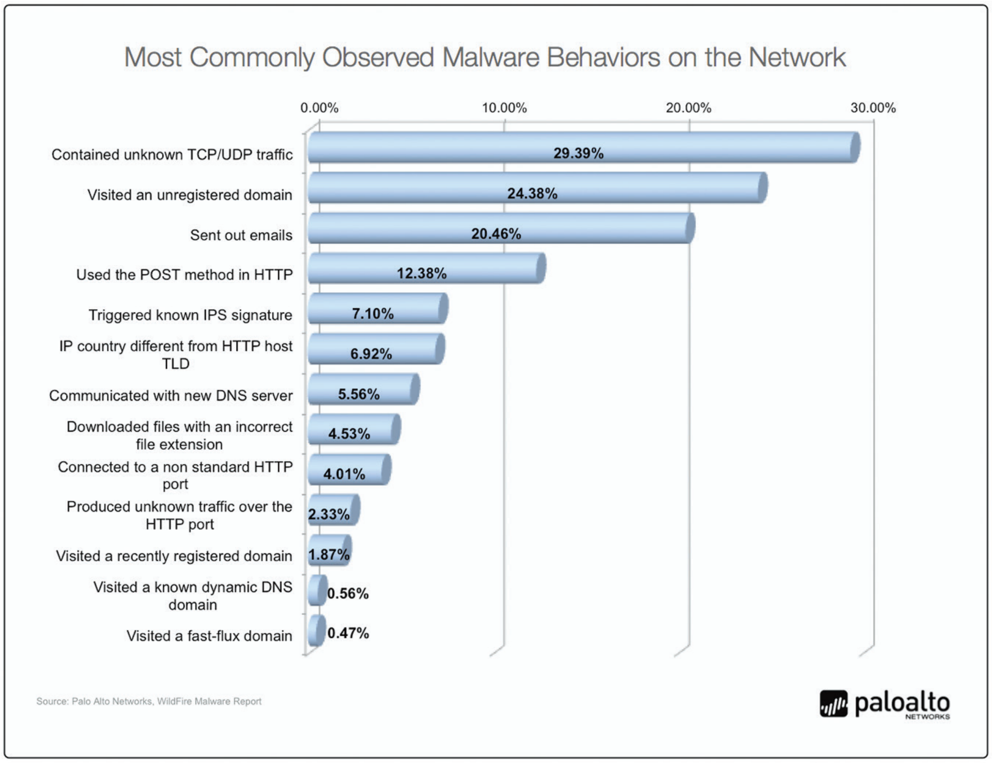
One of the most common malware indicators was the use of customized traffic by malware.

One of the most common malware indicators was the use of customized traffic by malware. Malware will often customize well-known protocols for their own purposes. This may include modifying standard protocols such as HTTP or DNS, but peer-to-peer, instant messaging and remote desktop protocols and applications are common targets as well. Any type of application that provides communication, resilience and the ability to transfer files is potentially valuable to malware.

Since the next-generation firewall positively classifies all traffic, its relatively easy to identify custom or unknown traffic in the network. Complementary studies in the Palo Alto Networks Application Usage and Threat Report have clearly shown a strong correlation between custom traffic and malware, and that trend held true in this study. Custom TCP and UDP counted as one of the most commonly identified behaviors observed in malware, as well as some of the most commonly generated traffic overall.

- 30% of unknown malware samples generated unknown traffic. This was the 4th most common malware behavior out of more than 100 observed behaviors.

- Custom/Unknown Traffic was the 3rd most common traffic type behind only web-browsing and DNS.



Most Commonly Observed Malware Behaviors on the Network

Source: Palo Alto Networks, WildFire Malware Report

While security teams may not want to block all traffic to and from a new domain, they may want to enforce tighter controls such never allowing executables from these sites.

SUSPICIOUS MALWARE TRAFFIC

In addition to looking at the actual malware traffic, it is often helpful to look at where the malware is coming from and going to. Identifying domains and sites that have served malware has been a long-standing component of URL filtering solutions. To stay ahead of these solutions, malware operators will generate custom domains for the attacks, use large numbers of essentially disposable domains, as well as dynamic DNS and fast-flux domains in order to avoid be blocked. As part of the analysis we tracked the number of samples that connected to these domains as well as samples that connected to known malware sites.

- **33% of samples connected new domains, DNS or fast-flux:** Newly registered domains, fast-flux domains and dynamic DNS can be also be blocked or blocked in conjunction with custom traffic or other indicators.

- **20% of samples generated emails:** These samples were observed direct email connections over the network. As a result, network policy should only allow email protocols to and from the corporate mail server, and block direct email to the Internet.

- **12% used HTTP-POST:** HTTP-POST methods are very common in malware, but are also often used by web-applications. As a result, teams will likely not want to block HTTP-POST altogether, but it may make sense to block going to unregistered or newly registered domains.

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

The analysis showed that while malware may be unknown to traditional security solutions, identifiers still remain. These identifiers can present in the payload of the malware itself or in the network traffic that the malware generates. Some indicators can be conclusive on their own, while others may be best used in conjunction with additional indicators. The suggestions below, should be used as general guidance, but will obviously need to be customized to the realities of a particular network.

- **Stream-based analysis of file headers and payloads for malicious indicators:** Needless to say that recognizing and blocking variants of malware in real-time is far preferable to detecting a remediating. The data shows that at least 40% of unknown malware were observable variants. This puts a very high priority on analyzing the actual malware payload, and timely delivery of newly identified malware intelligence.

- **Establish and update a solid baseline for the network:** Malware behaviors are often (but not always) anomalous, and these behaviors can be used to root out unknown malware quickly. However, malware techniques and strategies will always change, and as such it is critical to know what is normal for your network as opposed to the industry in general. A detailed baseline can provide the point of reference that exposes malware.

- **Investigate and remediate unknown traffic:** Unknown or custom traffic can be several things in addition to malware. As part of establishing a baseline, security teams should seek out unknown traffic and identify it conclusively going forward. It should quickly be possible to reduce the amount of unknown traffic to very low levels, where malware can easily be identified.

- **Restrict rights to unknown, newly registered domains and dynamic DNS domains:** The Internet is obviously a dynamic place, and it may not be that uncommon to encounter an unclassified or new domain. So while security teams may not want to block all traffic to and from a new domain, they may want to enforce tighter controls such never allowing executables from these sites, decrypt SSL traffic for inspection, or blocking HTTP-POSTs to these unknown sites.

- **Only allow email traffic to the corporate email server:** A significant number of malware samples generated email directly to destination on the Internet. This is very common behavior among spamming botnets, and behavior that can be easily controlled. Email traffic that does not go to the corporate email server can be easily blocked, and any users sending such traffic can be investigated as a potential malware infection.

MALWARE TRAFFIC ON NON-STANDARD PORTS

Non-SSL traffic on port 443 was the most common non-standard port behavior.

Malware was observed sending traffic over non-standard ports in both inbound and outbound traffic. The prevalence of this non-standard behavior varied widely by application as shown below. Using non-standard ports can allow malware to evade some security measures, which look for specific types of threats on particular ports. Non-SSL traffic on port 443 was the most common non-standard traffic behavior. This makes sense given that port 443 is almost always allowed on a network, and some organizations will not inspect traffic on 443 assuming that it is encrypted.

The section below provides a summary of some of the more significant types of malware traffic including the relative use of non-standard ports:

FTP

FTP was one of the most interesting and concerning applications that we observed in the course of the report. It was the 4th most common source of unknown malware, the malware it delivered was rarely detected (average of 30 days out of 31), and almost always operated on a non-standard port. FTP is of course very flexible and light-weight, making it a powerful tool for attackers that may not get the attention it deserves from security teams.

FTP was the most evasive application in terms port evasion, and had one of the lowest detection rates in terms of malware.

- Observed FTP traffic on 237 non-standard ports (neither side of the connection using port 20 or 21).
- 97% of malware FTP sessions went over non-standard ports.
- Led all applications in terms of non-standard behavior.

WEB BROWSING

Web-browsing was the workhorse application for unknown malware throughout the lifecycle. It was #1 source of malware, and the #1 type of traffic generated by malware. It was also observed to be one of applications used extensively for downloading additional payloads to the host. Malware delivered by web-browsing took 20 days on average in order to gain coverage. However, web-browsing on non-standard ports was relatively rare, accounting for only about 10% of sessions and 14% of bandwidth.

- Observed web traffic on 90 non-standard web ports (server operating on a port other than port 80).
- Relatively uncommon, accounting for only 10% of malware web-browsing sessions.
- Use of non-standard ports was slightly higher for browsing sessions that downloaded data. Non-standard ports accounted for 14% of downloaded bandwidth related to web browsing.

CUSTOM AND UNKNOWN TCP AND UDP

Custom traffic was predictably heavily tied to the traffic generated by the malware itself. Custom traffic was the 3rd most common traffic type after web-browsing and DNS. The use of non-standard ports varied considerably between TCP and UDP, with about half of unknown TCP using seemingly random ports and UDP staying on well-known ports.

- Observed custom TCP traffic on 19 non-standard ports (server operating on a port other than web, mail or proxy ports).

- 43% of unknown TCP traffic was observed on ports not associated with any well-known applications.

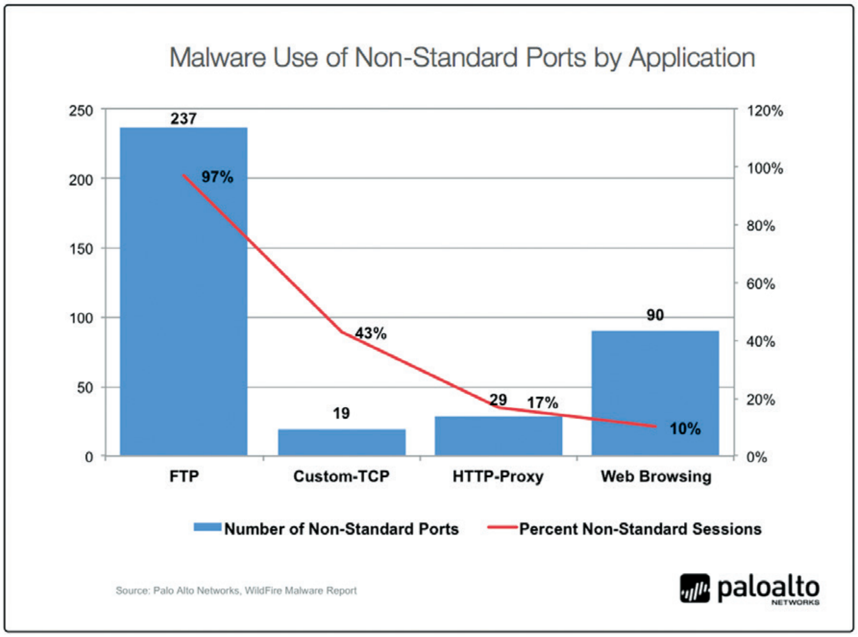
- Conversely, custom-UDP was found exclusively on well-known ports 53, 80, and 443.

HTTP PROXY

HTTP-Proxy traffic was the 2nd most common source of unknown malware after web-browsing. Proxies showed behavior very similar to web-browsing in terms of time to detection, requiring 19 days for coverage on average. Proxies were more likely to use non-standard ports that simple web-browsing (17% for proxies, 10% for web-browsing).

- Observed HTTP-Proxy traffic on 29 non-standard web ports (server operating on a port other than port 80, 443, 1080, 3128, 8000, 8080).

- Accounted for 17% of malware http-proxy sessions.



Source: Palo Alto Networks, WildFire Malware Report

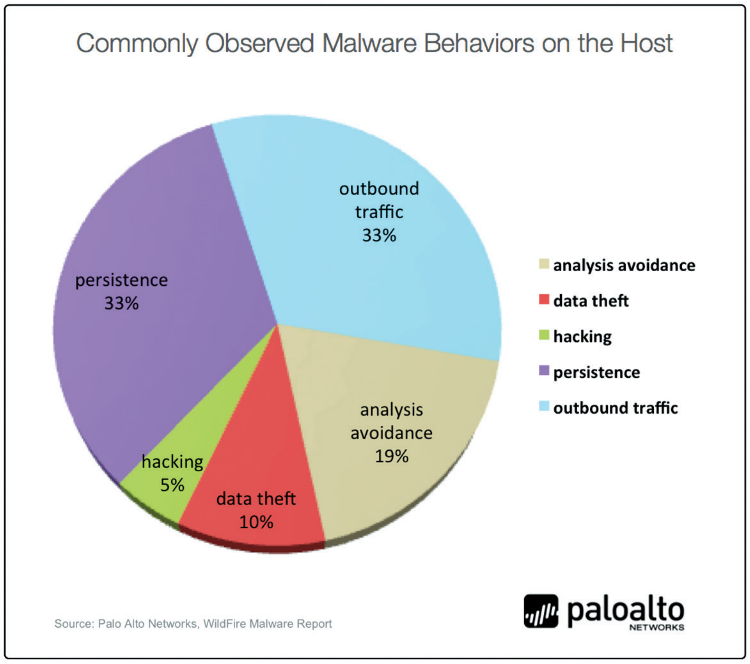
MALWARE BEHAVIORS ON THE HOST

Needless to say, a great deal of the malware life-cycle is focused on the infected host. Malware must be able to persist on the target for it to be useful in a long-term attack, and this requires the malware to blend in on the host while avoiding or disabling any security measures present. In total, behaviors designed to avoid analysis and persist on the host accounted for more than half of the behaviors observed by malware.

As part of analyzing potential malware, WildFire will execute a sample file and observe it for more than 100 malicious or suspicious behaviors. These behaviors have been broadly categorized as follows:

- **Analysis Avoidance:** Specific steps to avoid analysis either in a malware sandbox or other security solution (e.g. attempt to sleep for a long period of time).
- **Persistence:** This includes a variety of tasks required for the malware to exist on the host for long periods including how the malware will be run the host and avoid host-based security.
- **Hacking:** These behaviors are directed outside of the infected host and typically involve fingerprinting the surrounding network, and identifying nearby vulnerable hosts.
- **Data Theft:** Traffic that is specifically observed stealing information from the compromised host such as passwords or simply device configuration information.
- **Outbound Communication:** Includes malware command-and-control and a variety of behaviors referenced in the previous section concerning malware traffic

The table below shows the percentage of behaviors observed in each category.


Commonly Observed Malware Behaviors on the Host

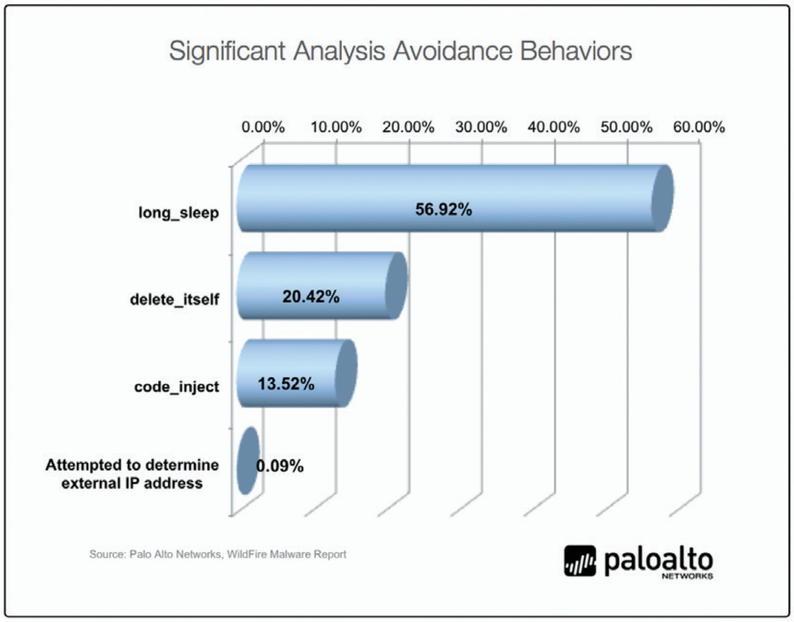
Source: Palo Alto Networks, WildFire Malware Report

The attempt by the malware to sleep (avoid executing initially to avoid attention) was the most common avoidance behavior and also the most common behavior overall regardless of category.

ANALYSIS AVOIDANCE

Analysis avoidance behaviors were some of the most common behaviors observed, yet were the least diverse. In short, we observed a handful of techniques in a large percentage of samples. The attempt by the malware to sleep (avoid executing initially to avoid attention) was the most common avoidance behavior and also the most common behavior overall regardless of category. Code injection was observed in 13.5 percent of samples. This technique is notable in particular because it allows malware to hide within another running process. This has the effect of the malware out of view if a user checks the task manager and can also foil some attempts at application white-listing on the host.

While quite rare, it was interesting to see malware that attempted to check its external IP address. This likely indicates an attempt by the malware to determine if it is truly in the target network or if its network connection is being proxied.

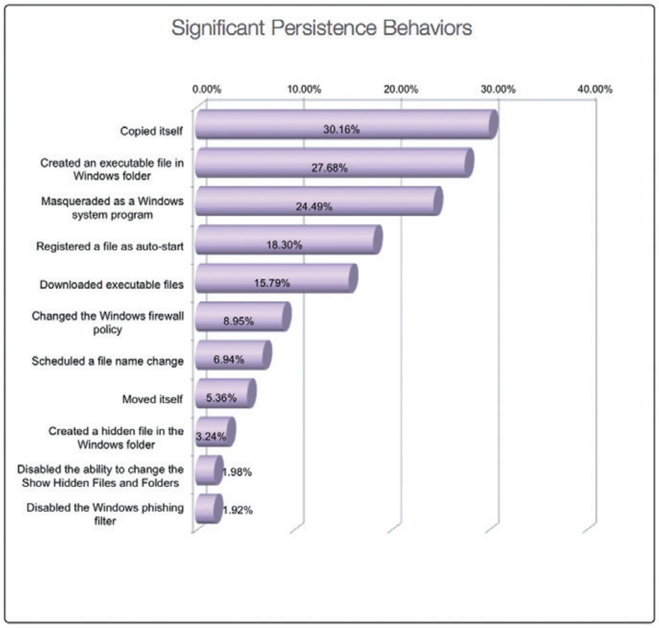


Source: Palo Alto Networks, WildFire Malware Report

PERSISTENCE

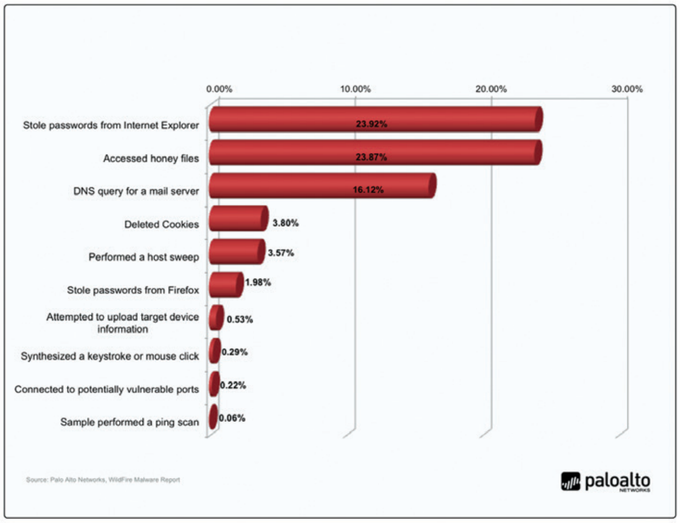
The Persistence category was one of the most active categories of behaviors as malware employed a wide variety of techniques to remain embedded on the host. In all WildFire observed more than 26 persistence behaviors. Common strategies where to invade or overwrite key components or directories of the operating system, configuring the malware to run automatically when the host is booted up and disabling host security components.

Some behaviors were rare, but still quite notable. A small number of samples were observed to infect the Master Boot Record, which is a key requirement for a bootkit. Other rare but interesting behavior altered the host to prevent a system restore, ensuring the infected system couldn't be rolled back to a good state. Other modifications included tampering with operating system to allow files to be run even with invalid signatures.


Significant Persistence Behaviors

HACKING AND DATA THEFT

While persistence and avoidance are means to an end, hacking and data-theft are the ends. Predictably, this category was highly varied in terms of observed behaviors. Given the preponderance of malware delivered via web-browsing, it was not surprising to see the browser as a common target. Theft of passwords stored in the browser and manipulation of cookies were both common behaviors.



Source: Palo Alto Networks, WildFire Malware Report

SUMMARY

Malware has become the key enabler for modern sophisticated attacks due to its ability to avoid traditional antivirus solutions, and provide a persistent internal foothold for long-term information attack once inside. As attackers and malware evolve, so to must our security responses. Modern malware presents a unique challenge in that the most sophisticated attacks will continue to require trained and diligent security professionals to investigate and analyze. On the other hand, the sheet volume of unknown malware can easily overwhelm even well-staffed security teams. As a result, security must aggressively seek out methods to automate the blocking of unknown malware wherever possible, while actively investigating the unknowns that get through. This report has hopefully provided some insight into the nature of the unknown malware problem, and provided some basic steps that security teams can use to protect their networks.

ABOUT PALO ALTO NETWORKS

Palo Alto Networks is the network security company. Its next-generation firewalls enable unprecedented visibility and granular policy control of applications and content—by user, not just IP address – at up to 20Gbps with no performance degradation. Based on patent-pending App-ID™ technology, Palo Alto Networks firewalls accurately identify and control applications—regardless of port, protocol, evasive tactic or SSL encryption—and scan content to stop threats and prevent data leakage. Enterprises can for the first time embrace Web 2.0 and maintain complete visibility and control, while significantly reducing total cost of ownership through device consolidation. Most recently, Palo Alto Networks has enabled enterprises to extend this same network security to remote users with the release of GlobalProtect™ and to combat targeted malware with its WildFire service. For more information, visit www.paloaltonetworks.com.

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Main: +1.408.573.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com