WHITEPAPER

Beware of the 64-bit Malware

May 2017

A deep dive into the 64-bit Windows operating system threat landscape

#1
Executive summary

The 64-bit Windows operating system is increasing its market share and becoming the prevalent system in most business environments. Its growing popularity is also attracting more attackers and slowly reshaping the Windows threat landscape. Cybersecurity teams must gain a deep understanding of 64-bit systems, and the different malware variants that can infiltrate and attack them, especially as the threat expands into additional operating systems, such as Linux and macOS.

This paper is the result of Deep Instinct's detailed research into the 64-bit Windows operating system threat landscape. It provides a comprehensive overview of the current state of 64-bit malware in the wild, analyzes the trends and sets out forecasts. This white paper will provide cybersecurity research teams and management with a solid foundation for developing awareness to potential attacks.

Upon Reading this White Paper, Cybersecurity Teams Will Learn:

- ✓ Why it is important to understand the architecture of the 64-bit operating system?
- ✓ What are the main differences between 64-bit and 32-bit operating systems, and how do they affect susceptibility to malware?
- ✓ What is 64-bit malware and why is it a growing threat to your organization?
- ✓ Which directions is the 64-bit threat landscape heading to?

#2

Introduction: The 64-bit threat landscape

64-bit Windows operating systems are gaining an increasing market share, and currently hold a clear majority of the operating system market. Despite the high proportion of 64-bit users, 64-bit malware still makes up less than 1% of the current threat landscape. However, as malware variants have recently begun to appear in 64-bit versions, this number is expected to grow. This paper will highlight relevant characteristics of 64-bit systems with regards to malware threats, and will then review the evolution of 64-bit malware and the current state of the 64-bit threat landscape. As very few publications have thoroughly discussed this topic, this paper is one of the first to review the risk of 64-bit malware, and the challenges posed by it to the cybersecurity industry.

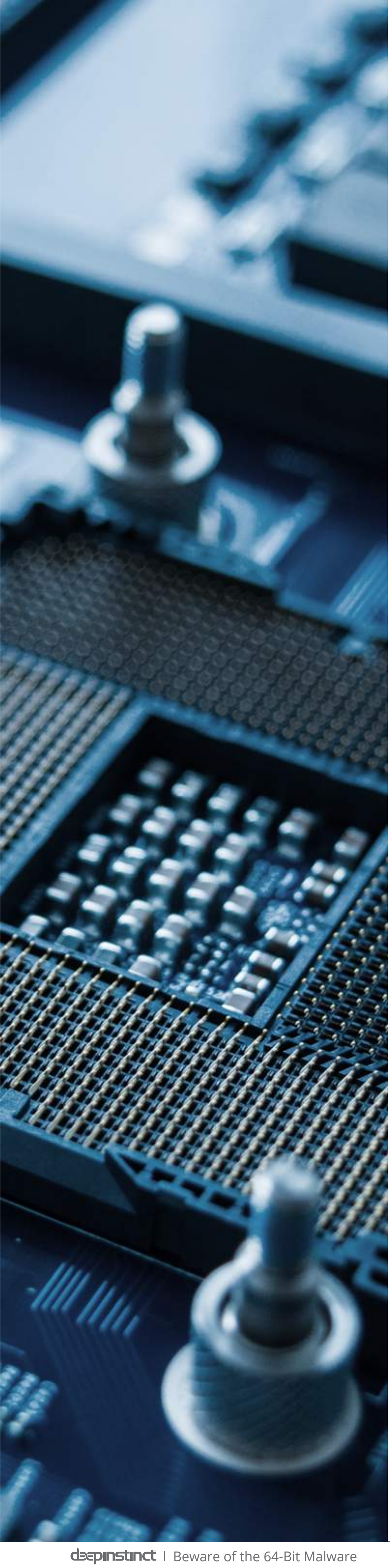
Quick Facts

- 92.8% of new computers sold worldwide operate on 64-bit Windows.[1] We expect that as users continue to transition to 64-bit operating systems and applications, so will malware authors.
- Over the past two years many well-known malware families, such as several ransomware and banking Trojan families, began using 64-bit variants in addition to 32-bit variants. Zeus, the leading banking Trojan, which is responsible for the theft of hundreds of millions of dollars, was the first of its kind to contain a 64-bit version. We expect other banking Trojans and ransomware to follows this trend, causing the numbers of 64-bit malware to increase in the coming years.
- Sophisticated 64-bit malware has already appeared in several APT campaigns. Notably, the destructive disk-wiping Shamoon malware, which destroyed data on 35 thousand computers at Saudi Aramco, has recently utilized 64-bit variants in a new wave of destructive attacks. We expect state-sponsored actors to use more 64-bit tools, as their targets will transition to 64-bit operating systems and applications.
- The 64-bit threat landscape is far less fragmented than its 32-bit counterpart, with several specific malware variants dominating.
- Recent studies and reviews have shown the cyber-security industry faces serious challenges in detecting malicious 64-bit files.

[1] http://news.softpedia.com/news/Microsoft-Explains-Why-Windows-10-32-Bit-Is-Still-Needed-469563.shtml

#3

Understanding 64-bit systems



The key differences between 32-bit and 64-bit machines

There are several significant differences between 32-bit and 64-bit machines. The most important difference lies in the fact that processes and operating systems running on 64-bit machines have substantially more virtual memory available – those operating systems hold 16 TB of virtual memory (which is only a fraction of the theoretical amount of virtual memory that is available for 64-bit systems), while 32-bit machines can hold a maximum 4 GB. This enables 64-bit machines with a suitable operating system to efficiently access and manage more than 4 GB of physical memory[2], while running larger numbers of processes and applications simultaneously.
In addition, 64-bit processes offer potentially better performance, as all addresses and pointers are 64 bits instead of 32. Furthermore, programs in 64-bit systems have more available handles.

In Windows environments, 64-bit PE files (with the magic PE32+) also have some key structural differences when compared to the older PE32 files. First, the format has been extended to encompass the memory space now available to a 64-bit application. Second, structural differences in the format affect the PE optional header, the import lookup/address table, the export address table and the TLS directory, while informational differences appear in three key fields: the machine signature, the size of optional header, and the optional header signature[3].

Running 32-bit applications on a 64-bit Windows system:

32-bit applications can run on 64-bit systems through the WOW64 (Windows-on-Windows-64) functionality, which provides backwards-compatibility for 32-bit applications installed on 64-bit Windows.

However, there are some important points to consider in this regard:[4]

1. In 64-bit Windows, 32-bit code must be isolated from 64-bit code. For this reason, 64-bit Windows systems have two registries: one for 64-bit code and one for 32-bit code. Since 32-bit code and 64-bit code cannot be combined, everything related to a 64-bit application, including the DLL files, must be 64-bit.
2. Any time a 32-bit application needs to read or write anything to or from the \Windows\System32 folder, the WOW64 emulator transparently redirects the request to the \Windows\SysWOW64 folder, as the System32 folder is used as a repository for 64-bit DLL in 64-bit Windows.

It is important to note that no forwards compatibility is provided in 32-bit Windows service packs or updates, which means that 64-bit applications cannot run on 32-bit Windows.

[2] Kumar, E. U. (2010). User-mode memory scanning on 32-bit & 64-bit windows. *Journal in computer virology*, 6(2), 123-141.

[3] Microsoft Portable Executable and Common Object File Format Specification, Revision 10 (2016).

[4] https://blogs.msdn.microsoft.com/ashishme/2009/04/01/32-bit-vs-64-bit/

Despite the backwards compatibility provided by WOW64, some 32-bit code will not run under a 64-bit Windows operating system. For example, some 32-bit applications will not even install on a 64-bit operating system because many 32-bit applications use a 16-bit Setup program, and 64-bit Windows versions do not support 16-bit code. 32-bit code that should be executed at the kernel level also cannot be used, so all kernel-level code must be 64-bit, and 32-bit code must run at the user level so that it can be serviced by the WOW64 subsystem.

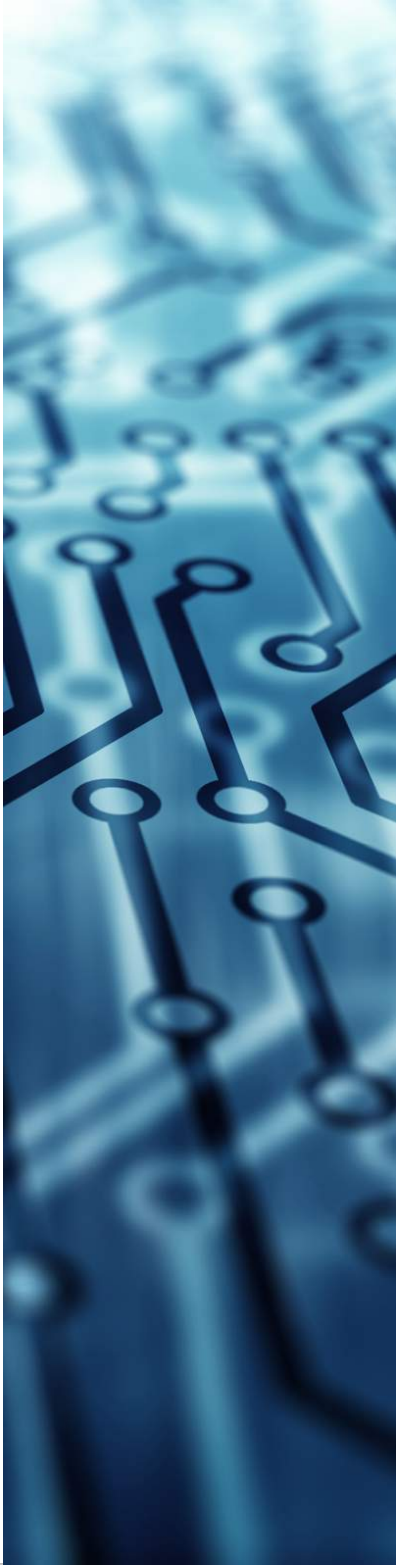
Moreover, 32-bit device drivers are not allowed to run – all drivers must be 64-bit, and must be digitally signed by their developers[5]. Despite the user being able to disable driver signature enforcement, this security measure caused a very noticeable drop in rootkits in the wild[6], however it was eventually bypassed by the TDL-4 (Alureon) rootkit, which was the first to bypass the blocking.[7]

In addition, there are several methods which enable unintended interaction between 32-bit applications running under the WOW64 system and 64-bit applications. For example, there is a tool which allows 32-bit applications running under the WOW64 system to read, write and enumerate memory of a x64 applications.[8]

Furthermore, there are several advanced techniques, which allow the execution of 64-bit system calls from a 32-bit application – the most well-known of which is Heaven's Gate, first described in 2009.[9] In a nutshell, Heaven's Gate enables a switch from 32-bit compatibility mode to 64-bit mode, within the WOW64 environment, and is used mostly as an anti-reversing mechanism. This switch is made from a specific segment – called Heaven's Gate[10] – that allows the bypassing of many security solutions. Since its first description, Heaven's Gate was adopted by many well-known malware families. For example, it has recently been implemented by the Scylex banking Trojan[11], while in the past it was adopted by another banking Trojan, Vawtrak.[12] Surprisingly, despite being in the wild for several years, this technique is relatively uncovered by mainstream cyber-security media.

Another difference is that driver-signing and the kernel "PatchGuard" protection make it extremely hard to infect 64-bit systems with rootkits. In addition, despite the ideal attack surface provided by WOW64 for 32-bit malware, it is very difficult for 32-bit malware running on a 64-bit system to access the memory of 64-bit processes.[13]

The growing number of 64-bit operating systems and applications shows that malware authors will need to utilize 64-bit malware if they wish to exploit 64-bit processes. However, as can be seen in the next section of our analysis, 64-bit malware remains extremely scarce, and the threat landscape is still dominated by 32-bit malware.



[5] http://searchwindowsserver.techtarget.com/tip/The-lowdown-on-64-bit

[6] http://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2016.pdf

[7] https://www.virusbulletin.com/uploads/pdf/conference_slides/2010/Johnson-VB2010.pdf

[8] https://github.com/rwfpl/rewolf-wow64ext

[9] http://vxheaven.org/lib/vrg02.html

[10] http://rce.co/knockin-on-heavens-gate-dynamic-processor-mode-switching/

[11] https://heimdalsecurity.com/blog/security-alert-scylex-financial-malware-crime-kit/

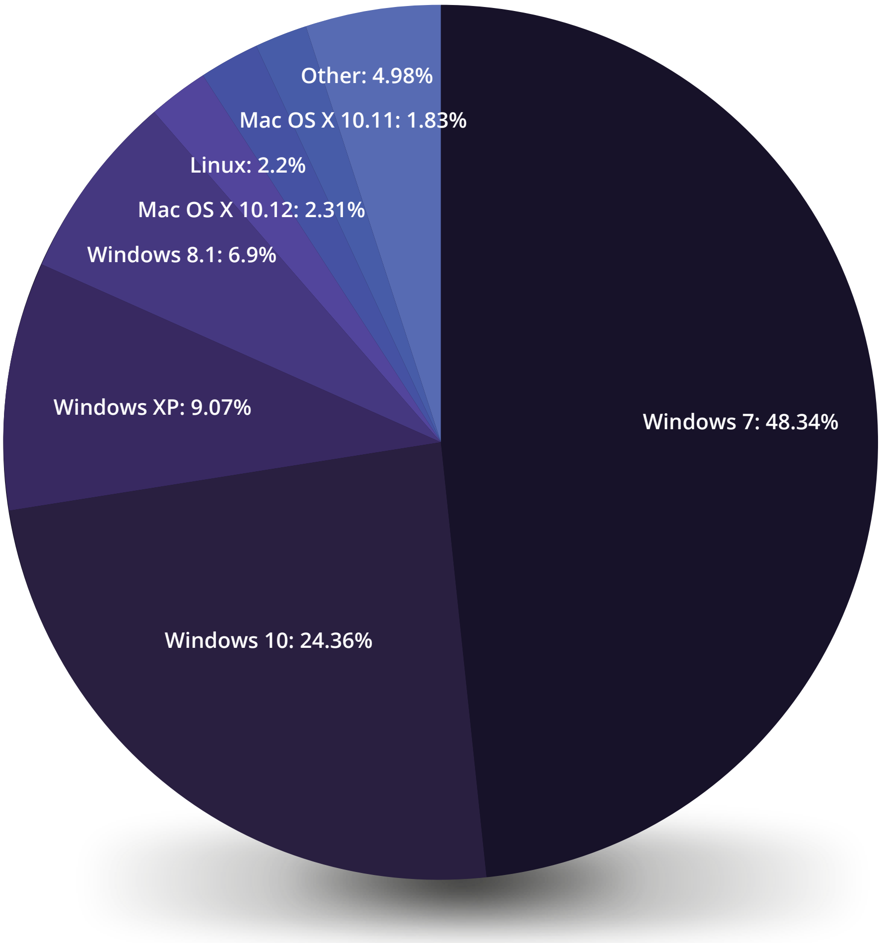
[12] https://int0xcc.svbtle.com/notes-on-vawtrak-banking-malware

[13] https://duo.com/assets/pdf/wow-64-and-so-can-you.pdf

The market share of Windows 64-bit operating systems

Based on the recent market share of 64-bit Windows systems, it can be safely assumed that 64-bit hardware and operating systems are now the first choice for home and business users alike. Back in 2009 Gartner predicted that by 2014 75% of corporate PCs will run 64-bit Windows,[14] and already as early as 2010, almost half of all installed Windows 7 editions were 64-bit[15]. In January 2015, a Microsoft executive, stated that 92.8% of new computers sold worldwide are 64-bit Windows.[16] In the gaming world, 64-bit Windows 10 became the most popular version in April 2016, passing Windows 7 for the first time. According to the survey conducted by Steam, 85% of Steam users use 64-bit Windows versions.[17] In addition, Unity hardware statistics show that since 2015 users have been gradually adopting 64-bit, and as of January 2017 80% of Unity users use 64-bit Windows.[18] Furthermore, a recent wide survey of one weeks' worth of browser data revealed that 84% of browsers execute on a 64-bit system, while only 16% execute on 32-bit systems.[19] All this leads to the conclusion that 64-bit Windows systems make up a large majority of the operating system market share.

The current operating system market share



The current operating system market share
Source: https://netmarketshare.com/

[14] http://www.digitaltrends.com/computing/most-corporate-pcs-to-run-64-bit-windows-by-2014-says-gartner/
[15] https://blogs.windows.com/windowsexperience/2010/07/08/64-bit-momentum-surges-with-windows-7/#msksz6kcLVlxIK3K.97
[16] http://news.softpedia.com/news/Microsoft-Explains-Why-Windows-10-32-Bit-Is-Still-Needed-469563.shtml
[17] http://www.digitaltrends.com/computing/steam-users-windows-10-market-share/
[18] http://hwstats.unity3d.com/pc/os-win.html
[19] https://duo.com/assets/pdf/wow-64-and-so-can-you.pdf

#4
64-bit malware

Why write 64-bit malware?

While both 32-bit and 64-bit applications can be run on a 64-bit system, in most cases 32-bit code cannot access the memory of a 64-bit process. In addition, malware which wishes to run malicious code inside a 64-bit process must, in most cases, be written as a 64-bit application[20]. There are multiple reasons for a malicious actor to exploit 64-bit applications. These can be specific vulnerabilities in the application, which could grant the attacker access to other parts of the system, information processed or held within the application; evasion of security solutions through injection into a 64-bit process; or knowledge of specific attributes in the victim's environment that make 64-bit malware more likely to achieve infection and its desired effect.

Currently the clear majority of malware variants in the wild are still 32-bit. This is due to the cross-architecture attack surface offered by the WOW64 back-compatibility, which means 32-bit malware can be used, in most cases, to attack both 32-bit and 64-bit operating systems. However, while many 32-bit malware variants can work on 64-bit systems, attacks demanding access to 64-bit process memory, such as code injection or privilege escalation attacks, will be much easier to undertake using 64-bit malware. Therefore, the threat landscape is expected to gradually shift to 64-bit malware, as 64-bit architectures and operating systems become the norm.

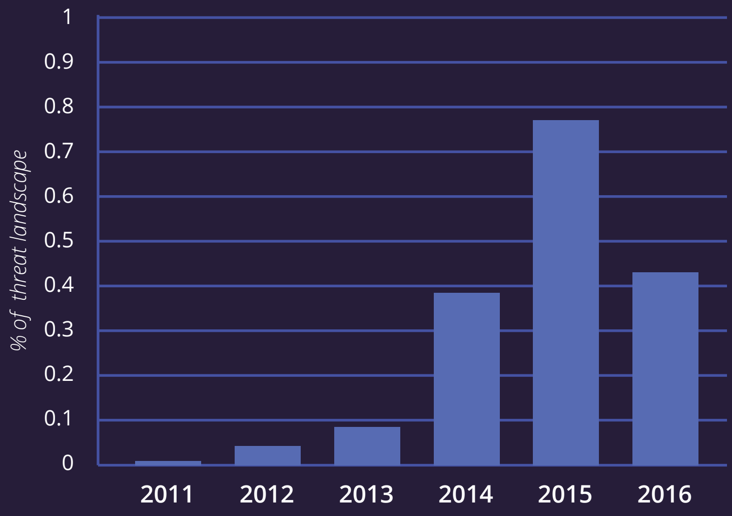
[20] http://searchwindowsserver.techtarget.com/tip/The-lowdown-on-64-bit

The evolution of 64-bit malware

In order to understand the 64-bit threat landscape, we conducted extensive research on 64-bit malware which appeared in the wild since 2011. During our research, several industry-recognized malware feeds were utilized, and over half a billion files were surveyed. Our research revealed several interesting findings:

Growth of 64-bit PE malware

Since 2011, the number of 64-bit malware underwent a 40-fold increase. Despite the great increase, 64-bit malware still makes up less than 1% of the PE threat landscape. The annual share of 64-bit malware from the total percentage of new malware variants since 2011 can be seen on the right. It can be seen that since 2011 the portion of 64-bit malware in the PE threat landscape has steadily increased until 2015, and then dropped in 2016. The 2016 drop was caused by a decrease of more than 50% in the spread of the most dominant 64-bit threat, Expiro.

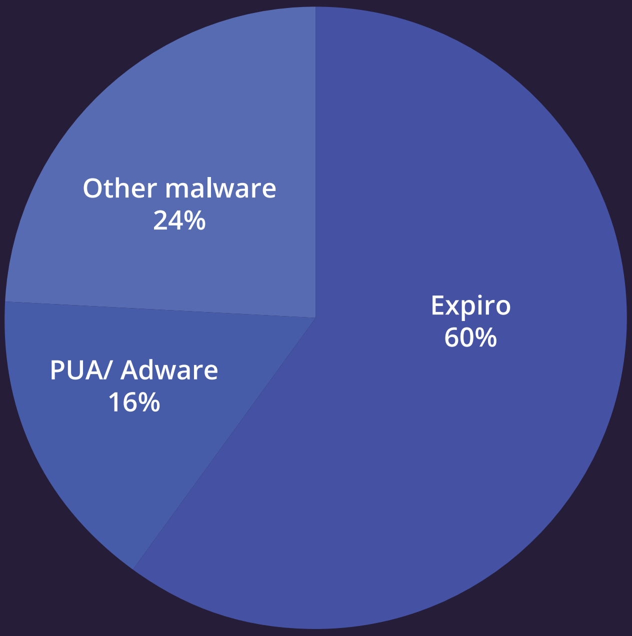


The growth of 64-bit PE malware in the wild since 2011. During the whole period 64-bit malware made up less than 1% of the annual threat landscape.

64-bit threats in the wild

Around 60% of the 64-bit threat landscape is dominated by the worm-like Expiro spyware, while the rest of the threat landscape is fragmented. The other main families, each making up around 2.5% of the threat landscape, are:

a. Patching Malware: variants which patch several Windows files and applications.
b. A family of AutoIt executables, which has many functionalities, predominantly bitcoin mining.
c. Bedep, a backdoor family.
d. Possibly Unwanted Applications, such as application download-bundlers, browser toolbars, or Adware, make up 16% of the 64-bit threat landscape.



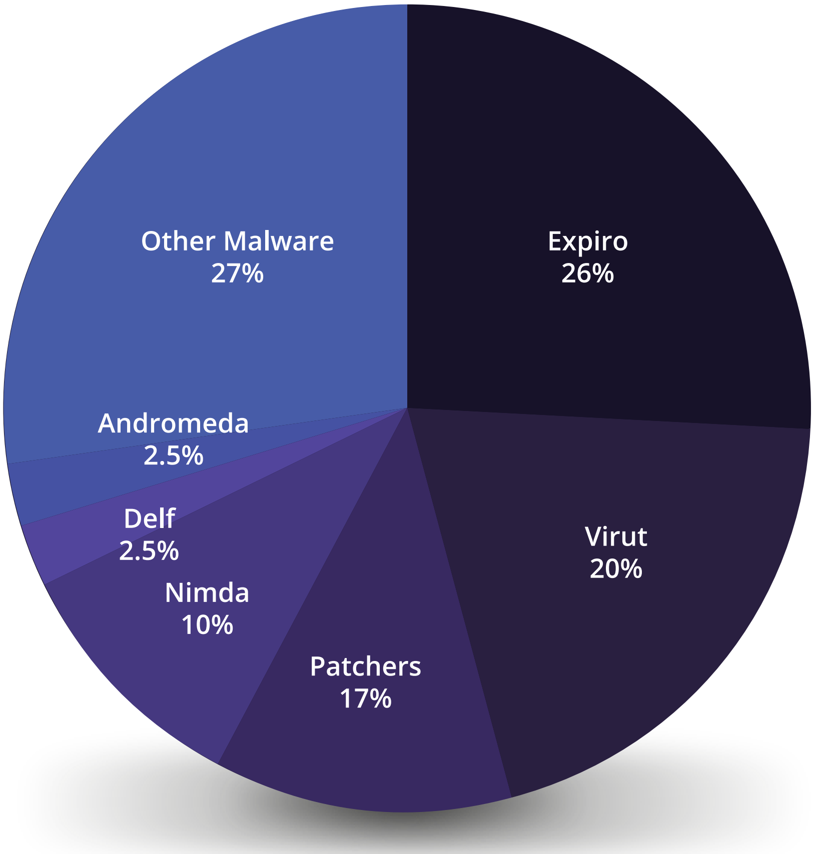
The 64-bit threat landscape, based on figures collected since 2011.

The state of 64-bit malware in the wild

We will now proceed to take a snapshot of the current state of 64-bit malware in the wild at the beginning of 2017.

While we can conclude that 64-bit malware is still less than 1% of the landscape, and the most common 64-bit malware remains Expiro, the share of this spyware-worm has significantly decreased compared to previous years (26% compared to 60%). However, other malware variants with worm-like propagation techniques still make up more than 50% of the observed malware samples. Apart from Expiro, the most common 64-bit families are Virut (20%) and Nimda (10%). The high prevalence of these worms in the threat landscape is unsurprising, as all of them infect files which in turn infect more files, and cause this type of malware to spread quickly and wide. The next most common type of 64-bit malware is a family of Trojans that patches Windows components (12%).

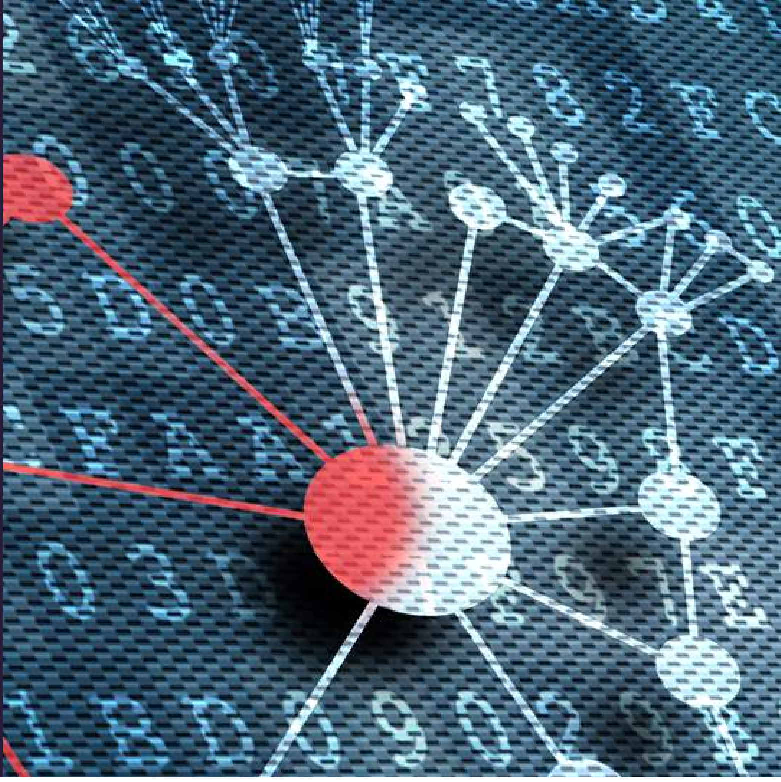
Current spread of 64-bit malware in the wild



The current 64-bit threat landscape, based on figures collected during January 2017.

A drill-down into the most common 64-bit malware families

A brief overview of the main characteristics of the most prevalent 64-bit Windows threats.



Expiro

A spyware which spreads in a worm-like fashion, and appears in both 32-bit and 64-bit variants. The 64-bit variant started to appear in 2013. Like other worms, Expiro infects executable files for propagation. However, in addition to infecting files on local drives, Expiro can also infect files on removable devices and network drives, quickly spreading itself to new victims. To reach a high number of victims, this spyware employs full cross-platform capabilities, as it possesses both 32-bit and 64-bit modules. There are several differences in the code for both modules – for example the entry point code size is different for both architectures, however the overall payload and action of the malware is identical. In order to steal information, Expiro employs several techniques, including installation of browser extensions, theft of stored certificates and passwords from several programs, and monitoring of HTTP traffic. Expiro was clearly created to spread quickly and far, and collect sensitive information from many computers. The 64-bit variants enable attackers to reach increasing amounts of 64-bit operating systems, while Expiro in general is a threat to both companies and home users, due to its information stealing capabilities.[21]

Virut

A common polymorphic backdoor with worm-like propagation that has 32-bit and 64-bit versions. This family of malware has many variants and acts as a backdoor by opening IRC communication with C2 servers, making the infected host part of a controlled botnet. The backdoor then enables the downloading of additional malware, and the authors of Virut receive payment through a pay-per-install (PPI) method with other malicious actors.[22]

The 32-bit version first appeared in 2006, and has since evolved greatly, as many new versions have been made by the developers of the virus.

[21] http://www.andrea-allievi.com/files/Expiro_Analysis_2013.pdf

[22] http://krebsonsecurity.com/tag/virut/

Patching Malware

A general name for malware variants which patch Windows files. This type of Trojan has several families, all of which have a similar functionality – they try to patch a Windows system file in order to divert its functionality. This patching can create many attack surfaces, and even create a functioning backdoor.

This family of Trojans also has 32-bit variants, which have an identical functionality and attack surface. The difference between both versions lies in the different path and name of some of the Windows system files patched by the two variants of the Trojans.

The most common malware of this type, a Trojan called Shopperz, appears to have surfaced in early 2015. This Trojan attempts to patch the dnsapi.dll, in an effort to override the Windows Hosts file, and load a modified Hosts file.[23] Since the patching of signed Microsoft files will most likely invalidate their signature, these Trojans can usually be detected by the presence of Microsoft files with an invalid signature. However, this is not always the case, as Deep Instinct has already demonstrated how malicious files can be hidden within signed files without invalidating their signature.

Nimda/Runouce/Chir

A worm which first surfaced in September 2001. The worm has 32-bit and 64-bit variants and utilizes several attack vectors: it can infect through email droppers, executable files, network shares, compromised web sites, and exploitation of old Microsoft vulnerabilities (this vector is no longer valid in most infection cases). This worm is widespread in both 32-bit and 64-bit systems.

Two other relatively common families of 64-bit malware are Delf (2.6%), a family of information stealers, and Andromeda (2.6%), a backdoor for the Andromeda botnet.

As can be seen, more than half of the historic and current 64-bit threat landscape is made up of worm-like malware. At least one of these malware variants, Expiro, is also spyware, and has actively been developed to work on 64-bit machines, in order to attack more targets. As Virut has been mutated by its developers many times, and works on a Pay-Per-Install arrangement, it can be assumed that this family was also actively changed by its developers in order to expand the possible attack surface and increase profit. As the number of 32-bit Windows users is constantly decreasing, we believe the amount of malware which aims to exploit 64-bit Windows will grow, and more types of malware will appear in the threat landscape.

[23] http://www.malekal.com/trojan-patched/

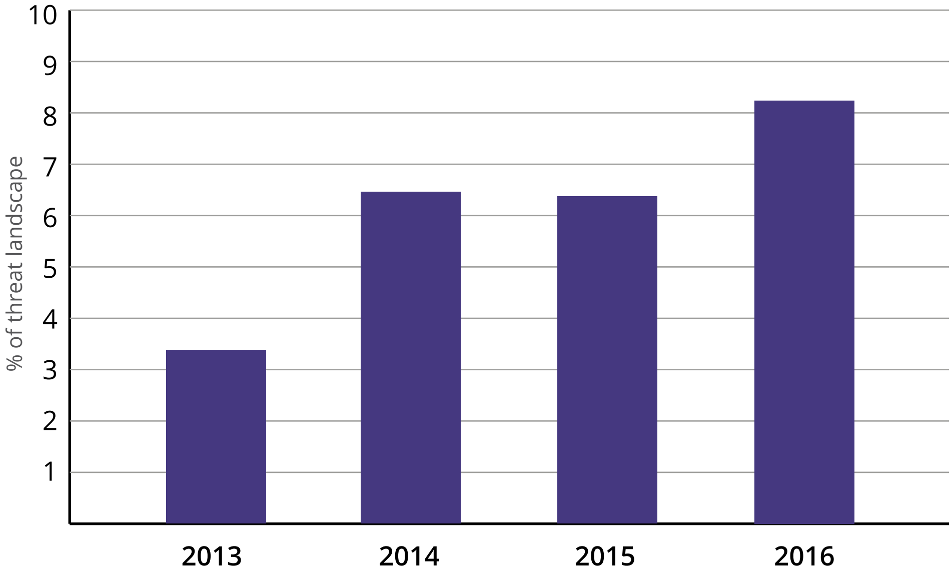
64-bit malware on Linux and macOS

Malicious 64-bit executables are not unique to Windows systems. This section will provide a short overview on the 64-bit threat landscape in Linux and macOS.

Linux

The Linux operating system is currently running on 2.2% of the desktop market,[24] and 12% of the server market.[25] Linux systems are available both in 32-bit and 64-bit forms. Linux malware, though still a rarity compared to Windows malware, has been on the rise in 2016. As of the end of 2016, 64-bit variants make up just less than 10% of the Linux threat landscape, but their levels in the wild have increased by 20% since 2015. end of 2016, 64-bit variants make up just less than 10% of the Linux threat landscape, but their levels in the wild have increased by 20% since 2015.

Growth of 64-bit Linux malware



The spread of 64-bit macOS malware variants in the wild since 2013.

Some notable Linux 64-bit malware variants are:

KillDisk: A disk-wiper which also has a ransomware version that targets Linux computers. The malware, which is attributed to the BlackEnergy group, also has a more known and researched Windows variant.[26]

Fysbis: A Linux-targeted trojan also attributed to a sophisticated attack group, Sofacy. The trojan has a modular structure which enables extensive data-theft, and is present both as a 32-bit and 64-bit ELF.[27]

[24] https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0

[25] https://community.spiceworks.com/networking/articles/2462-server-virtualization-and-os-trends

[26] https://www.bleepingcomputer.com/news/security/killdisk-ransomware-now-targets-linux-prevents-boot-up-has-faulty-encryption/

[27] http://resources.infosecinstitute.com/linux-malware-novelties-threat-landscape/#gref

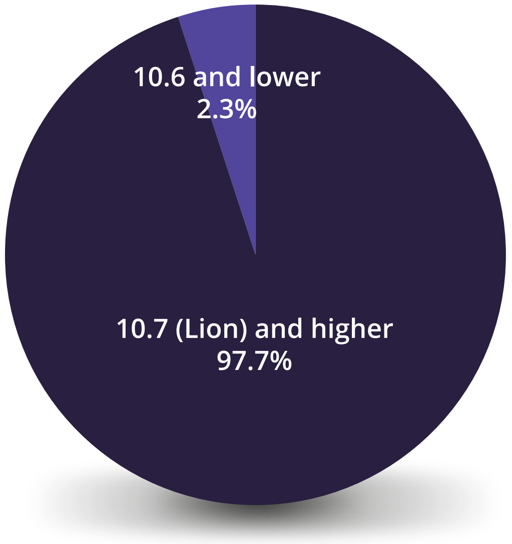
macOS

The macOS operating system holds an estimated 5-7% share in the desktop market.[28] The operating system also has 32-bit and 64-bit versions, however since macOS Lion (macOS 10.7), released in 2011, all new macOS platforms only run on 64-bit architectures. These platforms currently make-up 97.7% of the macOS market share.

It is also important to note that many macOS Mach-O executables are Fat binaries, meaning they support several different architectures, and as such, can run on different operating systems. For example, a Fat binary can have 32-bit and 64-bit code sections and will load the correct section into the operating system on which it runs.

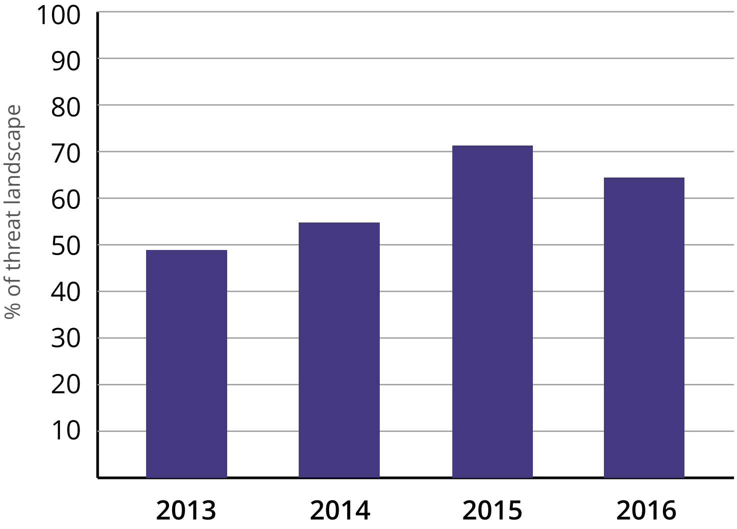
macOS malware was once a rarity, but has become increasingly more common in recent years. Malware that supports 64-bit architecture makes up the majority of the macOS threat landscape, which is unsurprising, as all macOS platforms since macOS Lion run only on 64-bit architectures.

macOS Distribution by Version



Current distribution of macOS by versions. All versions over and including macOS Lion (10.7) support only 64-bit architectures. Data adapted from https://www.netmarketshare.com/

Growth of 64-bit macOS malware



The spread of 64-bit macOS malware variants in the wild since 2013.

Examples of recent 64-bit macOS malware are:

KeRanger: The first fully functional ransomware which specifically targets macOS users. The ransomware spread through an infected version of the Transmission app, and demanded 1 Bitcoin from infected users in order to decrypt their files.[29]

Komplex: A Trojan created by the Sofacy group, to collect information from targets in the Aerospace industry. This Trojan has multiple versions, which can attack both 32-bit and 64-bit versions of macOS.[30]

[28] https://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0

[29] http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/

[30] http://researchcenter.paloaltonetworks.com/2016/09/unit42-sofacys-komplex-os-x-trojan/

#5 Detection of 64-bit malware

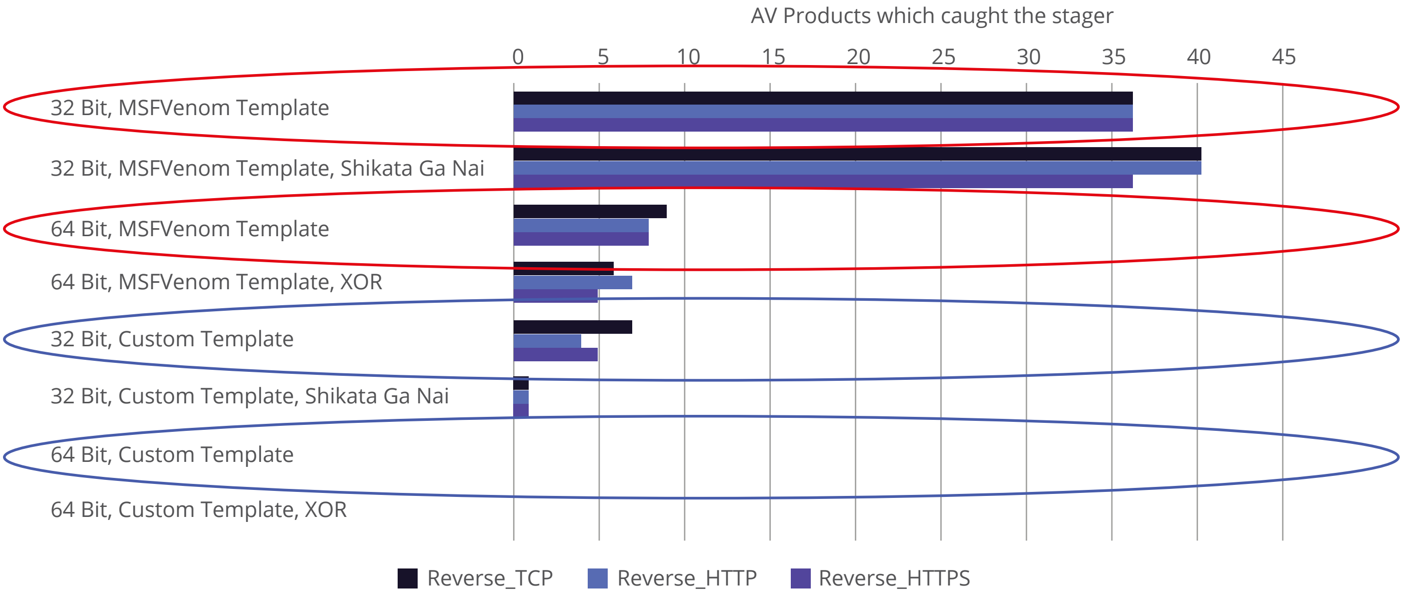
Detection of 64-bit malware

Several independent papers and articles have reviewed detection of 64-bit files. The tests presented in these studies show that the cyber-security industry underperforms on 64-bit files.

A paper presented in Black Hat 2014 tested the detection of 32-bit and 64-bit hacking tools by several leading AV vendors. According to the results presented in the paper, the use of 64-bit Meterpreter facilitates bypassing 10 out of 12 security solutions tested, while the usage of 32-bit Meterpreter was detected by all 12 products. This result was consistent with or without the use of packers.[31]

A more recent study, published in July 2016 [32], tested the detection rates of different Meterpreter stagers based on VirusTotal scan results. The results of the study can be seen in the following chart:

Meterpreter Stager Configurations Vs. Number of AV Detections



Adapted from: http://www.blackhillsinfosec.com/?p=5094

It can be seen that the detection rates for the 2 stagers, which have the same configuration in 32-bit and 64-bit (pairs marked in red and blue), are considerably lower for the 64-bit version of the stager.

A possible difficulty in detecting 64-bit files is the potentially lower number of heuristics for 64-bit files, possibly due to the lower number of 64-bit malware variants. One example for this was found in a blog post by the developer of NirSoft. According to the post, the 32-bit version of a NirSoft tool, WirelessKeyView, had 16 detections on VirusTotal, while the 64-bit variant, which is compiled from exactly the same code, has 0 detections.[33]

The tests and cases mentioned demonstrate the challenges 64-bit malware poses and the problems security providers face, given the smaller the threat landscape and reduced visibility to 64-bit threats. Considering the growing market share of 64-bit operating systems, the cyber-security industry will have to rise up to the challenge of accurately detecting and preventing 64-bit malware.

[31] Swinnen, A., & Mesbahi, A. (2014). One packer to rule them all: Empirical identification, comparison and circumvention of current antivirus detection techniques. BlackHat USA.

[32] http://www.blackhillsinfosec.com/?p=5094

[33] http://blog.nirsoft.net/2012/10/10/amazing-difference-between-antivirus-false-alerts-on-32-bit-and-64-bit-builds-of-exactly-the-same-tool/

#6 Conclusion: our predictions on the future of 64-bit malware

Our predictions on the future of the 64bit malware threat landscape

The detailed research set out in this white paper has led us to the following conclusions:

As users continue to transition to 64-bit, malware authors will follow:

Since the introduction of 64-bit operating systems for home and business users, there has been a gradual move to 64-bit operating systems. In line with this move, programs have begun to include 64-bit versions in addition to their older 32-bit version. In the beginning of 2015, a Microsoft executive claimed that 92.8% of new PC's are running Windows 64-bit versions.[34] This trend is expected to grow, and as users begin to use more 64-bit operating systems and programs, malware authors will want to reach these users, consequently, making 64-bit malware increasingly prevalent.

APTs will increase the use of sophisticated 64-bit tools:

Targeted attacks aimed at high value targets, which use specific 64-bit systems or applications will continue to be targeted by 64-bit malware that is tailor-made to attack them. As 64-bit tools also offer APT attacks higher stealth (because these types of attacks are usually state-sponsored or highly sophisticated, targeted ones), sophisticated actors will increase their use of these tools to evade detection. Furthermore, in the long term, as the prevalence of 64-bit operating systems and applications increases, the number of tools sophisticated actors use to target them is expected to increase as well.

Many APTs discovered in recent years included 64-bit malware:

BlackEnergy: a group which conducted several campaigns, including most notably an attack against Ukrainian critical infrastructure in late 2015.[35]

Winnti: a campaign which is believed to have been initiated in China, and targeted at least 35 companies primarily in South East Asia, Russia, Brazil, and the United States.[36]

Shamoon: a data-wiping campaign targeting government and industrial organizations in Saudi Arabia. In 2012, the Shamoon malware hit Saudi Aramco, wiping data from 35 thousand computers. In January 2017, a new strain of the malware, Shamoon 2, used 64-bit variants to damage numerous Saudi industrial and government organizations.[37]

[34] http://news.softpedia.com/news/Microsoft-Explains-Why-Windows-10-32-Bit-Is-Still-Needed-469563.shtml

[35] https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[36] https://securelist.com/analysis/internal-threats-reports/37029/winnti-more-than-just-a-game/

[37] http://researchcenter.paloaltonetworks.com/2017/01/unit42-second-wave-shamoon-2-attacks-identified/

The prevalence 64-bit malware will increase:

1. 2016 saw a massive unprecedented increase in the spread of ransomware. Despite that, there are currently relatively few ransomware samples which have 64-bit variants (for example CryptoWall, Reveton and Weelsof). To date, most ransomware variants are 32-bit files, and due to the WOW64 functionality in Windows, these files are able to attack 64-bit systems in addition to 32-bit systems. However, as users start using more 64-bit processes, and 32-bit operating systems will become less supported and common, ransomware writers will follow the trend and begin to write ransomware capable of attacking these exclusively 64-bit systems.
2. Like ransomware, banking Trojans have also become an increasing threat. This type of malware also includes 64-bit variants, to widen the scope of available victims, and increase the profit of the cybercriminals who created the malware. The most notable banking Trojan to “convert” to 64-bit is Zues/Zbot – with a 64-bit variant appearing in late 2013. Many other banking trojans followed suit, including Vawtrak and Dyreza.

About Deep Instinct

Deep Instinct is the first company to apply deep learning to cybersecurity. Leveraging deep learning's predictive capabilities, Deep Instinct's on-device, proactive solution protects against zero-day threats and APT attacks with unmatched accuracy. Deep Instinct provides comprehensive defense that is designed to protect against the most evasive unknown malware (including ransomware) in real-time, across an organization's endpoints, servers, and mobile devices. Deep learning's capabilities of identifying malware from any data source results in comprehensive protection on any device, any platform, and operating system. Deep Instinct is headquartered in Tel Aviv, Israel and has offices in San Francisco, CA. To learn more, visit: http://www.deepinstinct.com

www.deepinstinct.com

Deep Instinct Ltd.
23 Derech Menahem Begin, Tel Aviv, 66182 Israel +972 (3) 545-6600
501 Folsom Street, Suite 400, San Francisco, CA 94105, USA +1 (855) 522-2223