Email: Malware, spam & phishing

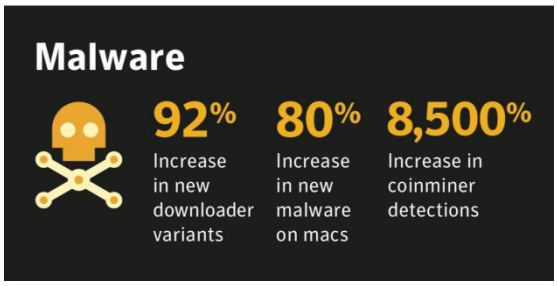
Authors：劉東亮　２０１６９４００５
張胤民　２０１６９４０６９
王宇晴　２０１６９４０８９

- **Internet Security in 2020**

1. Approaches of Web-Attack

1.1. Coin mining attacks explode

Cyber criminals who have been firmly focused on ransomware for revenue generation are now starting to explore other opportunities. During the past year, the astronomical rise in crypto currency values inspired many cyber criminals to shift to coin mining as an alternative revenue source.



With a low barrier of entry—only requiring a couple lines of code to operate—cyber criminals are using coinminers to steal computer processing power and cloud CPU usage from consumers and enterprises to mine crypto currency. While the immediate impact of coin mining is typically performance related—slowing down devices, overheating batteries, and in some cases, rendering devices unusable—there are broader implications, particularly for organizations.

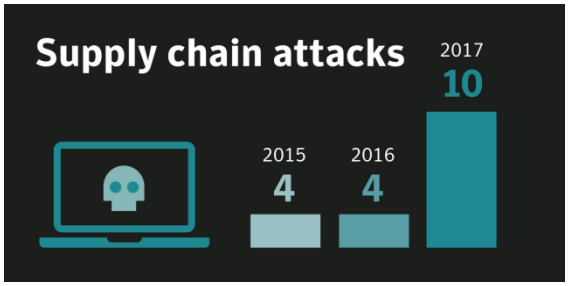
Corporate networks are at risk of shutdown from coinminers aggressively propagated across their environment. There may also be financial implications for organizations who find themselves billed for cloud CPU usage by coinminers.

As malicious coin mining evolves, IoT devices will continue to be ripe targets for exploitation.

1.2. Spike in software supply chain attacks

Despite the EternalBlue exploit wreaking havoc in 2017, the reality is that vulnerabilities are becoming increasingly difficult for attackers to identify and exploit.

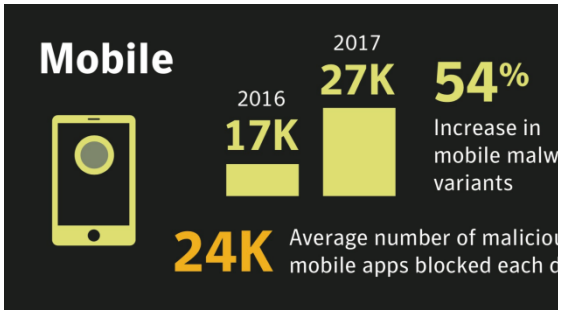
Hijacking software updates provides attackers with an entry point for compromising wellprotected targets, or to target a specific region or sector. The Petya/NotPetya outbreak was the most notable example: After exploiting Ukrainian accounting software as the point of entry, Petya/ NotPetya used a variety of methods, spreading across corporate networks to deploy the attackers' malicious payload.



1.3. Mobile malware continues to surge

Threats in the mobile space continue to grow yearover-year. The number of new mobile malware variants increased by 54 percent in 2017, as compared to 2016. And last year, an average of 24,000 malicious mobile applications were blocked each day.

While threats are on the increase, the problem is exacerbated by the continued use of older operating systems. In particular, on AndroidTM, only 20 percent of devices are running the newest major version and only 2.3 percent are on the latest minor release.



Mobile users also face privacy risks from grayware, apps that aren't completely malicious but can be troublesome. Symantec found that 63 percent of grayware apps leak the device's phone number. With grayware increasing by 20 percent in 2017, this isn't a problem that's going away.

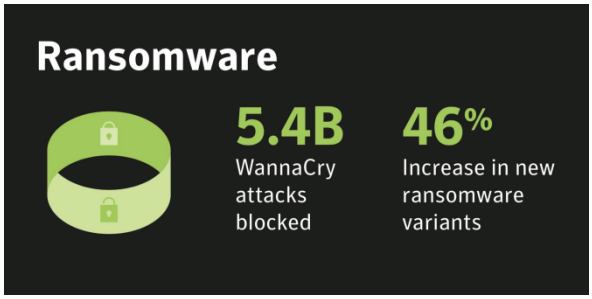
2. Ransomware business

Ransomware business experiences market correction

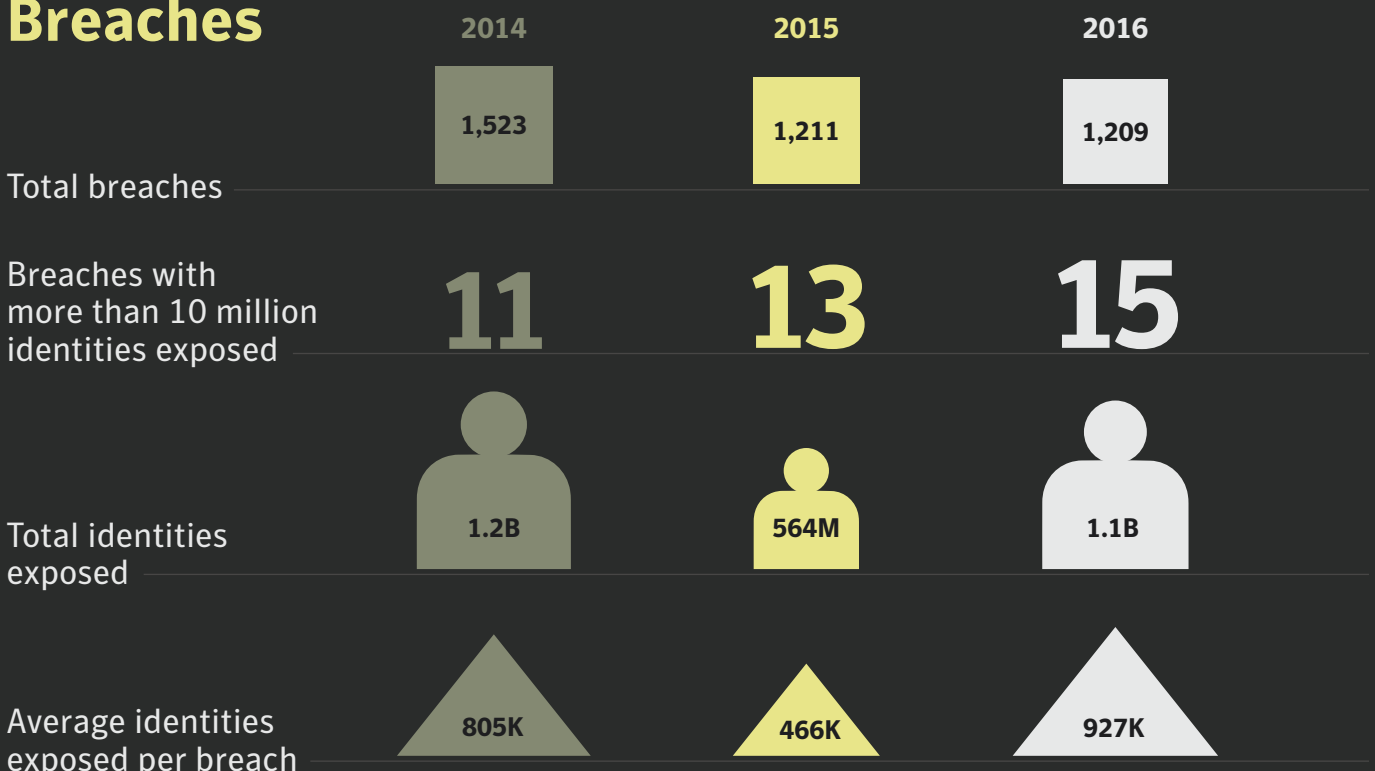
When viewed as a business, it's clear that ransomware profitability in 2016 led to a crowded market, with overpriced ransom demands. In 2017, the ransomware 'market' made a correction with fewer ransomware families and lower ransom demands—signaling that ransomware has become a commodity.

Many cyber criminals may have shifted their focus to coin mining as an alternative to cash in while crypto currency values are high. Some online banking threats have also experienced a renaissance as established ransomware group have attempted to diversify.

Last year, the average ransom demand dropped to $522, less than half the average of the year prior. And while the number of ransomware variants increased by 46 percent, indicating the established criminal groups are still quite productive, the number of ransomware families dropped, suggesting they are innovating less and may have shifted their focus to new, higher value targets.

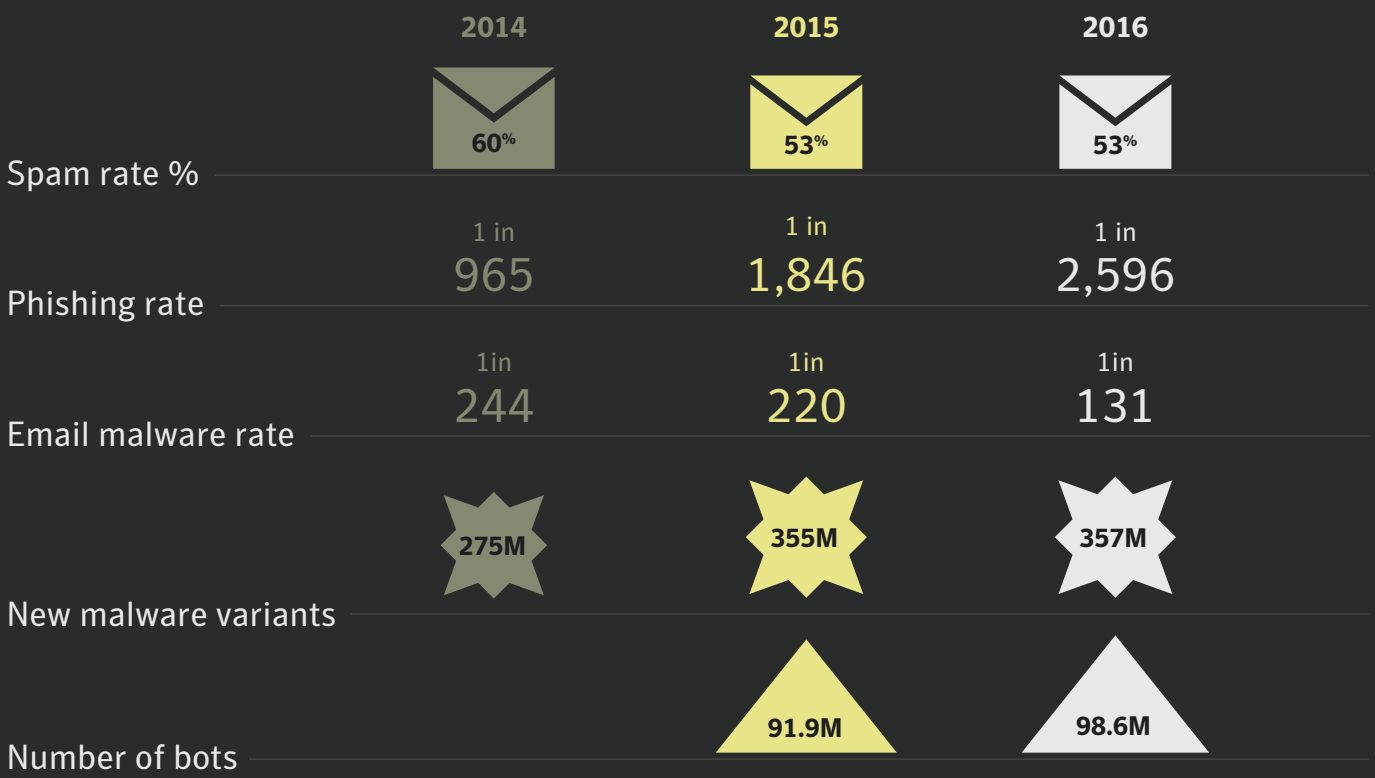


Breaches

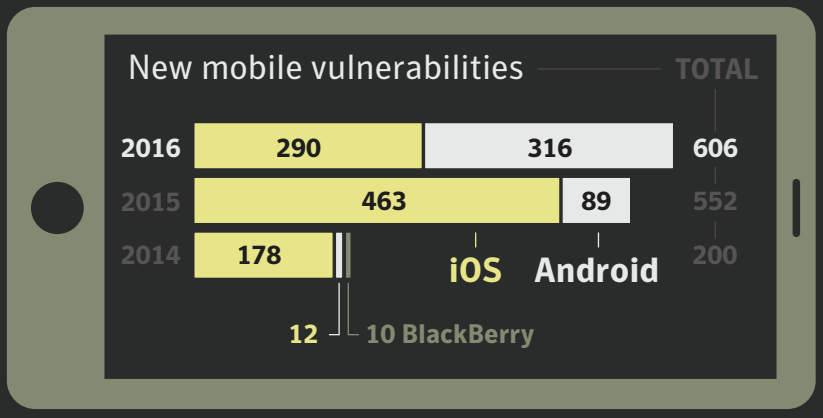


In the last **8** years more than **7.1 billion** identities have been exposed in data breaches

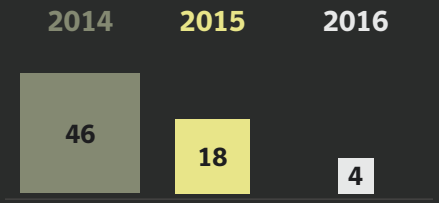
Email threats, malware, and bots



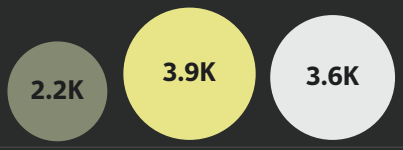
Mobile



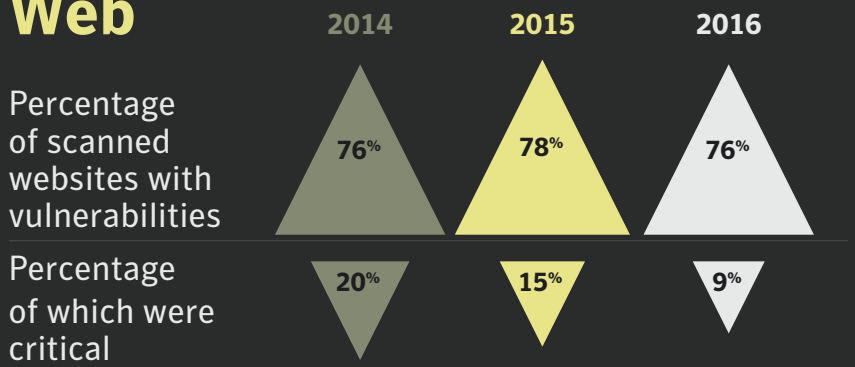
New Android mobile malware families



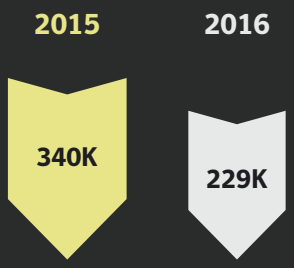
New Android mobile malware variants



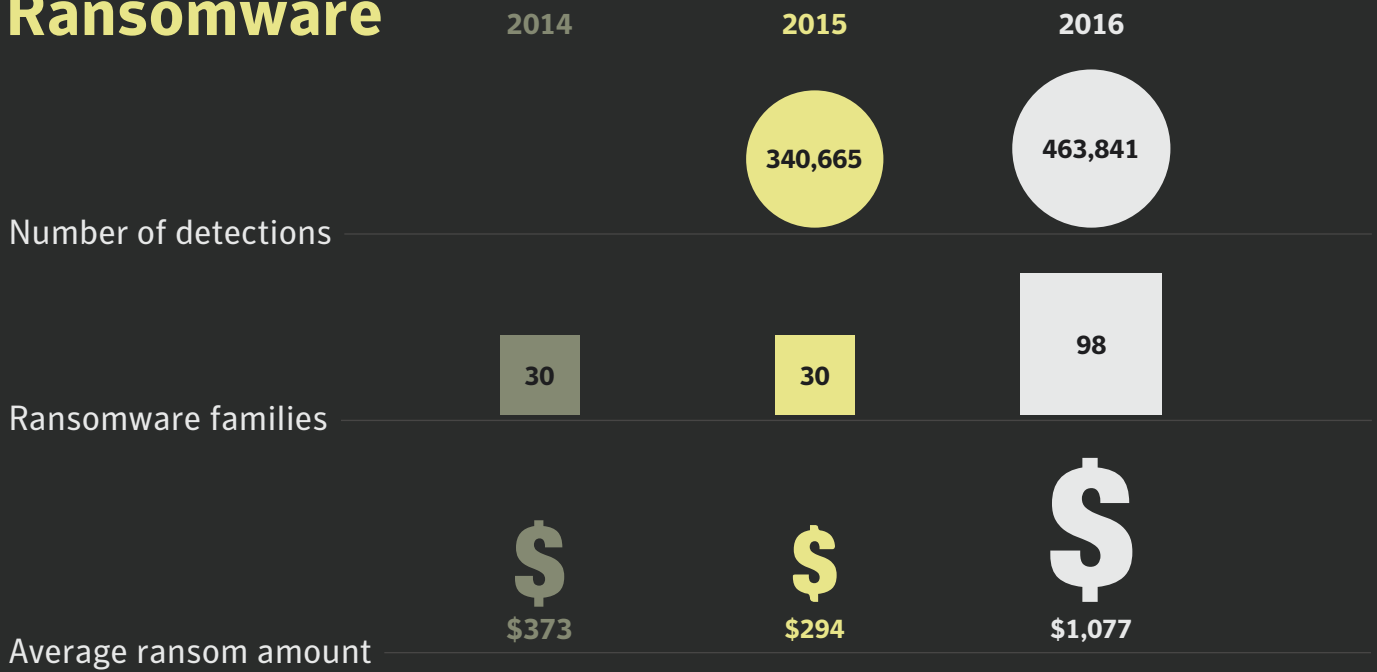
Web



Average number of web attacks blocked per day



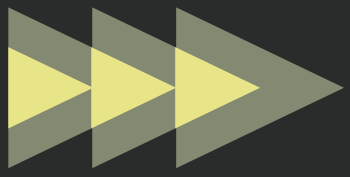
Ransomware



Cloud

	JUL-DEC 2015	JAN-JUN 2016	JUL-DEC 2016
Average number of cloud apps used per organization	774	841	928
Percentage of data broadly shared	25%	23%	25%

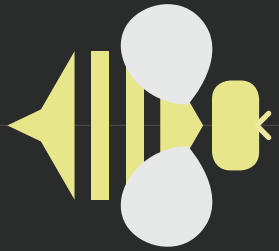
Internet of Things



Speed of attack

2 minutes: time it takes for an IoT device to be attacked

Number of attacks against Symantec honeypot **per hour**



JAN|**2016** DEC|**2016**

- Email: Malware, spam & phishing

1. Introduction

Although a vital communication tool, email is also one of the prime sources of disruption for end users and organizations. This disruption can range from unwanted emails in the form of spam to more dangerous threats, such as the propagation of ransomware or targeted spear-phishing campaigns.

IT systems continue to come under attack from rapidly evolving malware. Email remains the medium of choice for cybercriminals and email volumes continue to grow, as phishing and spam decline—the latter of which accounted for more than half of inbound email traffc. Phishing attacks were more targeted and malicious emails grew in number and complexity, highlighting how email remains an effective medium for cybercriminals

2. Key findings

The email malware rate increased significantly during 2016, from 1 in 220 emails sent containing malware in 2015, to 1 in 131 emails in 2016. This increase was driven primarily by botnets, which are used to deliver massive spam campaigns related to threats such as Locky (Ransom.Locky), Dridex (W32.Cridex), and TeslaCrypt (Ransom.TeslaCrypt).

Targeted spear-phishing campaigns, especially in the form of Business Email Compromise (BEC) scams, rather than the mass-mailing phishing campaigns of old, are now favored by attackers. This is reflected in the drop in phishing rates, which fell from 1 in 1,846 emails to 1 in 2,596 emails.

Major email threat groups are relying primarily on the use of first-stage downloaders to install their final payload, typically ransomware. At the beginning of 2016, Office documents containing malicious macros were the most common form of downloader being used in spam campaigns. However, a shift occurred in March and, since then, JavaScript downloaders have dominated.

Email continues to dominate digital communications, regardless of the rising popularity of instant messaging technology for both business and consumer use. There were approximately 190 billion emails in circulation each day in 2015, a number that we predict to grow by as much as 8 percent by the end of 2020. On average, each business user sent and received 42 emails each day, and a growing number of individuals were reading email on mobile devices. For cybercriminals who want to reach the largest number of people electronically, email is still the favored way to do it.

3. Malware menace

The most noteworthy trend observed through 2016 was the uptick in email malware rates. The rate jumped from 1 in 220 emails in 2015 to 1 in 131 emails in 2016

2014	2015	2016
1 in 244	1 in 220	1 in 131

Table1.Overall email malware rate

This increase in email malware can probably be linked to ongoing activity during 2016 by mass-mailing malware groups, primarily spreading Locky, Dridex, and TeslaCrypt. One of the major distributors of malware is a botnet known as Necurs (Backdoor.Necurs). Necurs is responsible for massive campaigns that spread malware through JavaScript and Office macro attachments. These downloaders subsequently install the final payload, which in 2016 was typically ransomware threats such as Locky

3.1. Necurs botnet

This is the tale of a cybercrime botnet operation that, within about five years of its existence, has been named one of the largest botnets in the world.

It’s called the Necurs botnet. It militarizes up to 6 million zombie endpoints, delivers some of the worst banking Trojans and ransomware threats in batches of millions of emails at a time, and it keeps reinventing itself. The bottom line is that Necurs is indirectly responsible for a major chunk of cybercrime and the losses it produces. According to reports, cybercrime

damages are expected to cost the world $6 trillion by 2021. This magnitude alone makes it worthwhile to get to know more about one the top players in that nefarious game.

3.2. Changes of malware rate

As is depicted in Fig2. The monthly email malware rate shows sharp drops in April and June, which may be linked to law enforcement activity against several cyber crime groups.

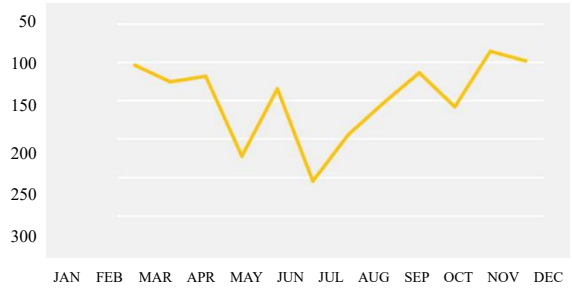


Figure1. Monthly email malware rate

3.3. Analyses

As it is described in Fig.1, this drop in activity may have been linked to law enforcement activity, with the drop in activity in June coming in the aftermath of the arrest of 50 people in Russia allegedly connected to the Lurk banking fraud group

However, this drop in activity was only temporary and malware spam campaigns quickly scaled up again. Campaigns involving Dridex and Locky resumed, while incidents of the Kovter family of threats (Trojan.Kovter) started increasing in August and maintained this growth for the rest of the year. For more details on mass-mailing ransomware campaigns, see our Ransomware chapter

3.4. Attacking targets

Email malware rate by industry Wholesale Trade and Agriculture were the classified industry sectors most affected by email-borne threats in 2016.

With the exception of Retail Trade, which saw a drop in its email malware rate (from 1 in 74 emails in 2015 to 1 in 135 emails in 2016), every industry saw an increase in email malware in 2016. The biggest increases were in the industries of Transport (from 1 in 338 emails to 1 in 176), Finance (from 1 in 310 to 1 in 182), and Mining (from 1 in 304 to 1 in 139). Healthcare Services saw a jump from 1 in 396 emails to 1 in 204.

Email malware hit businesses of all sizes in 2016. However, small- to medium-sized businesses (with 251 to 500 employees) were the most impacted, according to our figures.

Email malware rate by company size：The highest rate of malware in email traffic was in the 251-500 company size grouping, with 1 in 95 emails received containing malware.

Company Size	Email Malware Rate)
1-250	127
251-500	95
501-1000	139
1001-1500	224
1501-2500	104
2501+	170

Table2.Email malware rate by company size

3.5. Email Malware Trends

As with phishing fraud, malware distributed in emails requires social engineering to convince its recipient to open the attachment or to click on a link. Attachments can be disguised as fake invoices, office documents, or other files, and often exploits an unpatched vulnerability in the software application used to open that type of file. Malicious links may direct the user to a compromised website using a web attack toolkit to drop something malicious onto their computer.

The cybercriminal group behind this particular attack has used many different techniques for sending spam and malware: from simple malware attachments, hyperlinks in the message body that point to an exploit kit landing page, malicious PDF attachments, and document macros.

Email malware has not been in decline in the same way as general spam, and because of its relatively low volume in comparison, it is more subject to fluctuation. Spikes occur when large campaigns are undertaken.

Figure2. Typical emailed malware infection process

4. Resolutions

4.1. Remove Your Email Accounts redirect

- Uninstall Your Email Accounts from Windows
- Use Zemana AntiMalware Portable to remove Your Email Accounts New Tab
- Use Malwarebytes to scan for Adware and Browser Hijackers
- Double-check for malicious programs with HitmanPro
- (OPTIONAL) STEP 5: Reset your browser to the default settings

4.2. Remove Malware from Your PC

- Backup all your documents and files before you start removing the malware infection
- Enter your PC in Safe Mode with Networking
- Delete your temporary files
- Use these free malware removal tools
- Reset your browsing settings

4.3. Void installation of malware

To prevent this situation, be very cautious when browsing the Internet. Carefully analyze all received email attachments. Files that seem irrelevant or have been received from a suspicious/unrecognizable email address should never be opened. Have a legitimate anti-virus/anti-spyware suite installed and running. In addition, 2010 and newer versions of MS Office open newly-downloaded documents in "Protected View" mode. This prevents malicious documents from downloading/installing malware and, therefore, using older versions of MS Office is not recommended. The main reasons for computer infections are poor knowledge and careless behavior. The key to safety is caution. If you have already opened the "Job Applications Email Virus" attachment, we recommend running a scan with Spyhunter for Windows to automatically eliminate infiltrated malware.

4.4. Do protection measures after a malware infection

1. Use two-factor authentication management

system
2. Always keep your software up to date
3. Make sure you have an antivirus program installed
4. Use a traffic filtering solution to keep malware at bay

4.5. Use social engineering and new messaging platforms

As businesses and consumers move to newer messaging platforms beyond traditional email, attackers will likely seek to leverage these platforms for malicious purposes.

Businesses are increasingly using collaborative tools such as Slack for both internal communication and interactions with customers. In China, WeChat has dominated the messaging space, where it offers extensive features, including a payment system. Where financial transactions go, cyber criminals are likely to follow. WeChat will likely serve as a model for other messaging applications. Facebook Messenger has already increased its focus on the use of automated bots to allow brands to insert themselves into users' conversations.

While some of the techniques used in typical malicious emails are not transferable to other messaging platforms, at the root of email campaigns is the use of social engineering. The lessons learned from the success of email scams and campaigns will likely be applied to messaging platforms as they become more widely adopted by businesses and consumers.

5. References

[1] Protection measures after a malware infection. https://heimdalsecurity.com/blog/malware-removal/

[2] How to remove Your Email Accounts Redirect. https://malwaretips.com/blogs/remove-your-email-accounts/

[3] Avoid installation of malware. https://www.pcrisk.com/removal-guides/13428-client-requirements-email-virus

[4] How to remove malware manually. https://www.pcrisk.com/removal-guides/14077-thanksgiving-email-virus

[5]2016 Internet Security Threat Report https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[6] Internet attack https://baike.baidu.com/item/%E7%BD%91%E7%BB%9C%E6%94%BB%E5%87%BB/2412930?fr=aladdin

[7] Necurs Botnet, one of largest malicious architecture has vanished http://securityaffairs.co/wordpress/48248/cyber-crime/necurs-botnet.html