Seven ways Ransomware infects your network

MAYA
Business. Secure

Ransomware

Ransomware is a family of malicious code (malware) designed to encrypt files on a victim system and hold the encryption key(s) for ransom. Since its first appearance about eight years ago, ransomware has evolved. It acquired abilities such as worm-like propagation, C&C communication, evasion, data exfiltration and more but at its basic level – always the ability to encrypt files and demand ransom for decryption.

Some main reasons for ransomware being so prevalent are that infecting corporate networks is incredibly easy, many companies pay the ransom, and the chances for the attackers to get caught are slim.

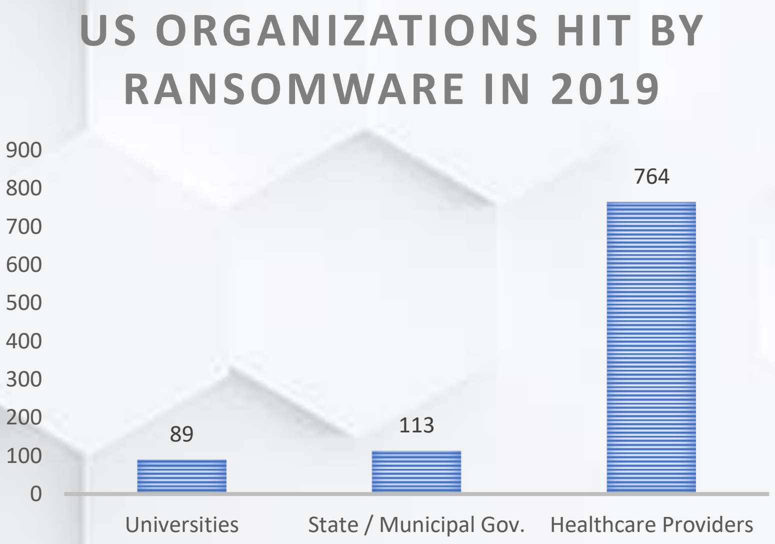
Ransomware has devastated countless networks with infamous ransomware attacks like *NotPetya* used against the Ukraine in 2017, *WannaCry* which crippled the UK health systems that same year, and of late – *REvil* which leaked documents belonging to Madonna, Lady Gaga and the president of the US.

National agencies and large enterprises usually bounce back after a ransomware attack due to sufficient budgetary reserves. For small and medium businesses – the situation is not as bright. According to research, almost 6 out of 10 SMBs which suffered a significant ransomware attack, went out of business within a year of that attack.

Winnebago County's Chief Information Officer, Gus Gentner, in a September statement: "**Statistics let us know that the average ransomware incident costs $8.1 million and 287 days to recover.**"

Knowing how ransomware infects your network (Attack Vector) can be the first step in avoiding most ransomware attacks.

Following are seven of the most common ways ransomware uses to infect networks.



Attack Vectors

1. Phishing

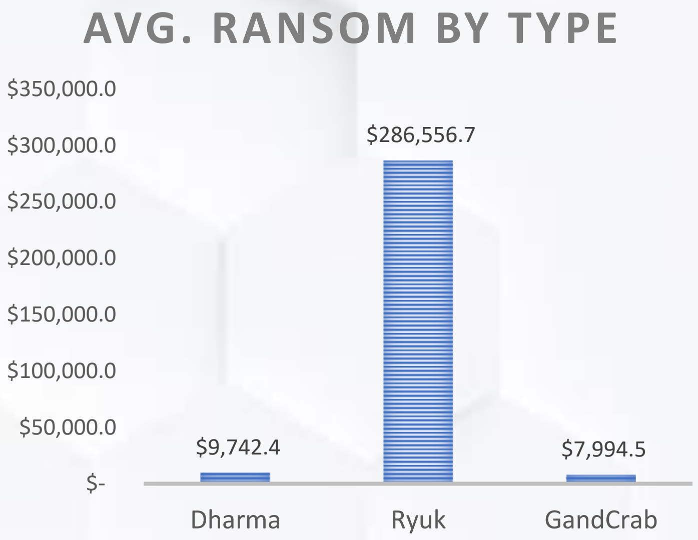
Path of Attack

Phishing and social engineering are still the most common methods of malware delivery. Attackers send an email message to millions of users, impersonating an official or familiar sender, urging users to click-open an attachment or click a link which in turn downloads and runs the malware. The result is an infected machine with encrypted files on it, attempting to further infect any other machine it can communicate with.

Phishing has evolved to spear-phishing, whaling and other methods that are specifically tailored to higher-value targets, making them even more difficult to identify and resist.

Mitigation

Employee awareness is arguably the best tool you can have in fighting phishing campaigns. As long as email remains a legitimate method of communication, attackers will use it to deliver malware. Resist-to-click is ultimately up to the employee as he or she faces the phishing email. As awareness to the dangers of phishing grows, the chances of employees clicking malicious links and attachments diminishes.



Credit: thenextweb.com

2. Compromised Websites

Path of Attack

A website or domain could be compromised in a few ways. Attacks like ‘Typosquatting’, ‘Combosquatting’, ‘Doppelganger Domain’, and many more Leuer an unsuspecting victim to a malicious website where malware is downloaded and installed on the victim’s machine (among other attacks).

Mitigation

Web redirections like this are particularly difficult for users to spot and so tools like cyber intelligence, IP & domain reputation, web filters and other tools are available to screen most of these malicious websites and domains out of your users’ reach.

Attack Vectors

3. Malvertising

Path of Attack

Websites depend on advertising for income and rely on third-party vendors to supply those ads. The ads are basically pieces of software running on the user's machine. Malicious ads can perform malicious activities like download and install malware on the victim's machine. We have seen malvertising campaigns run through legitimate websites like The New York Times and The Atlantic in 2018.

Mitigation

Since the user cannot verify every (or any) ad he or she view on a legitimate website, again – it is up to technology to save the day. Browser-based ad-blockers are a great way to limit ads (legitimate as well as malicious). Here too, IP and domain reputation filtering can help limit a malicious ad from downloading harmful payload by blocking its communication to the command and control server.

4. Exploit Kits

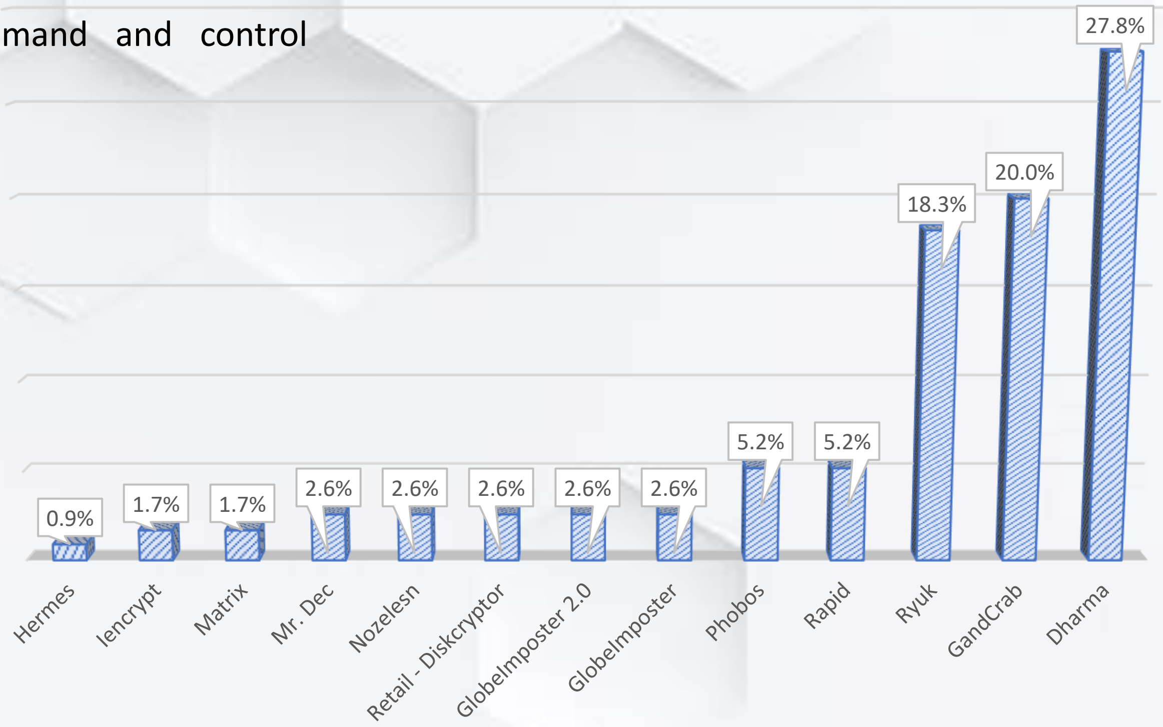
Path of Attack

Exploit kits are basically toolkits that combine several methods to exploit multiple vulnerabilities (in operating systems, third-party software, hardware etc.). Exploit kits are available for sale on the darknet and are used to spread ransomware. Maze ransomware is a good example as it was delivered by Spelevo exploit kit in late 2019, exploiting a vulnerability in Adobe Flash player.

Mitigation

As stated, exploit kits usually target known vulnerabilities and are successful against unpatched systems. Patching all operating systems and third-party software as soon as possible is a good way of blocking most exploit kits.

RANSOMWARE BY SHARE 2019



Attack Vectors

5. Files and Apps

Path of Attack

Users make use of corporate computers and network for work-related activities. Usually.

From the secretary's wedding photos to the marketing shadow-IT DropBox shared folder, employees introduce files and applications into the network. These unsanctioned files and applications can be infected images or infected pirated applications. These files and applications expose the network to cyberattacks, with ransomware being one of those attacks.

Mitigation

One way to fight this attack vector is employee awareness. In many cases, knowing the possible impact of introducing an unsanctioned file or application into the network, will prevent the employee from doing this in the first place.

Another way is ensuring all incoming content is going through a Content Disarm & Reconstruction (CD-R), ensuring only clean files enter the network.

Yet another mitigation method is application whitelisting which means that only approved applications are allowed to run in the network.

Businesses lose an average of 7.3 workdays to attacks, and an estimated $64,645 in additional downtime-related costs.

6. Instant Messaging

Path of Attack

An attack can disguise itself as a graphics file (SVG) to drop a malicious file while bypassing traditional file extension filters through instant messengers like WhatsApp and Facebook Messenger. The downloaded file can direct the unsuspecting user to a malicious website, execute a malicious file, and in this case – download the ransomware file and execute it.

Mitigation

See section above. Content filtering and cybersecurity awareness utilize both technology and informed employees' abilities to identify phishing attempts and block them.

Attack Vectors

7. Remote Access

Path of Attack

As teleworking becomes more prevalent, the connection between remote machine and the corporate network becomes more alluring to attackers who can easily find these ports through port scanners. Without restriction, attackers can hijack an RDP connection or brute-force their way into the network through an open RDP connection. Once inside the network, achieving admins privileges is a few hops away, allowing the attackers to install ransomware and exfiltrate sensitive data for extorsion purposes.

Mitigation

Patching is a must of course.

Then – making sure your open ports are not exposed to random scanning.

Also, hardening authorization processes like account lockout after 5 or 10 failed attempts, TFA or MFA, and many more may help fend off attackers.

FEDEX SAW A $300 MILLION LOSS DUE TO CYBERATTACKS. THE LOSS WAS NOT A RESULT OF PAYING THE RANSOM BUT PRIMARILY FOR THE COST OF DISASTER RECOVERY AND SYSTEM DOWNTIMES.

Being attacked may be inevitable.

Being helpless isn’t.

For more information on how to protect your company, email us today!

info@maya-security.com

* Sources: Emisoft
thenextweb.com
comparitech.com
phxtechsol.com

MAYA
Business. Secure