COMP482 Cybersecurity Week 2 - Wednesday

Dr. Nicholas Polanco

(he/him)

Attendance Poll

https://forms.office.com/r/z3qpXKT1eF

COMP482 - Attendance

Important Notes

1. You should go to SIP Fest today!
2. We have moved the project deliverable meeting to be the **Friday of Week 3 (April 18th)**.
    a. If you are working in a group and sending 1 representative, I will need all those group members to email me so I have something in writing that you approve of this.
3. Do we also want to move the topic presentation selection to that same **Friday of Week 3 (April 18th)**?
    a. This would only give you a week and a half to complete the presentation.
    b. However, you can submit a topic prior to that. Thoughts?

Important Dates (Week 2)

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
		Due: Think Like a Hacker Activity		Due: Recent Attacks Reflection 1 ~~Project "Idea" Meeting~~		

Malware

Malware

Malware (short for "malicious software") is any software intentionally designed to cause damage to a computer, server, or network, or to steal, corrupt, or compromise data. It can come in many forms, such as viruses, worms, Trojan horses, spyware, adware, and rootkits.

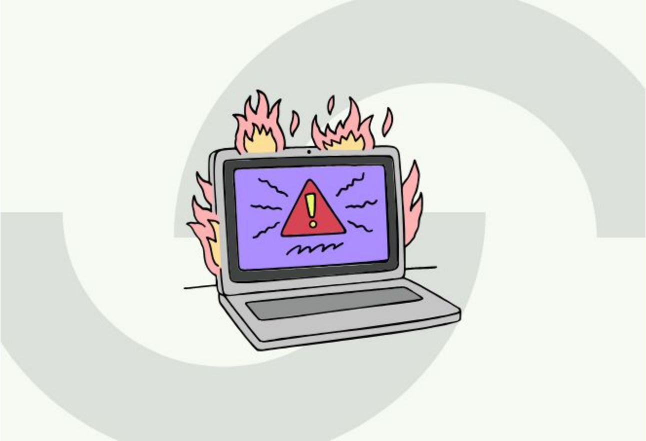


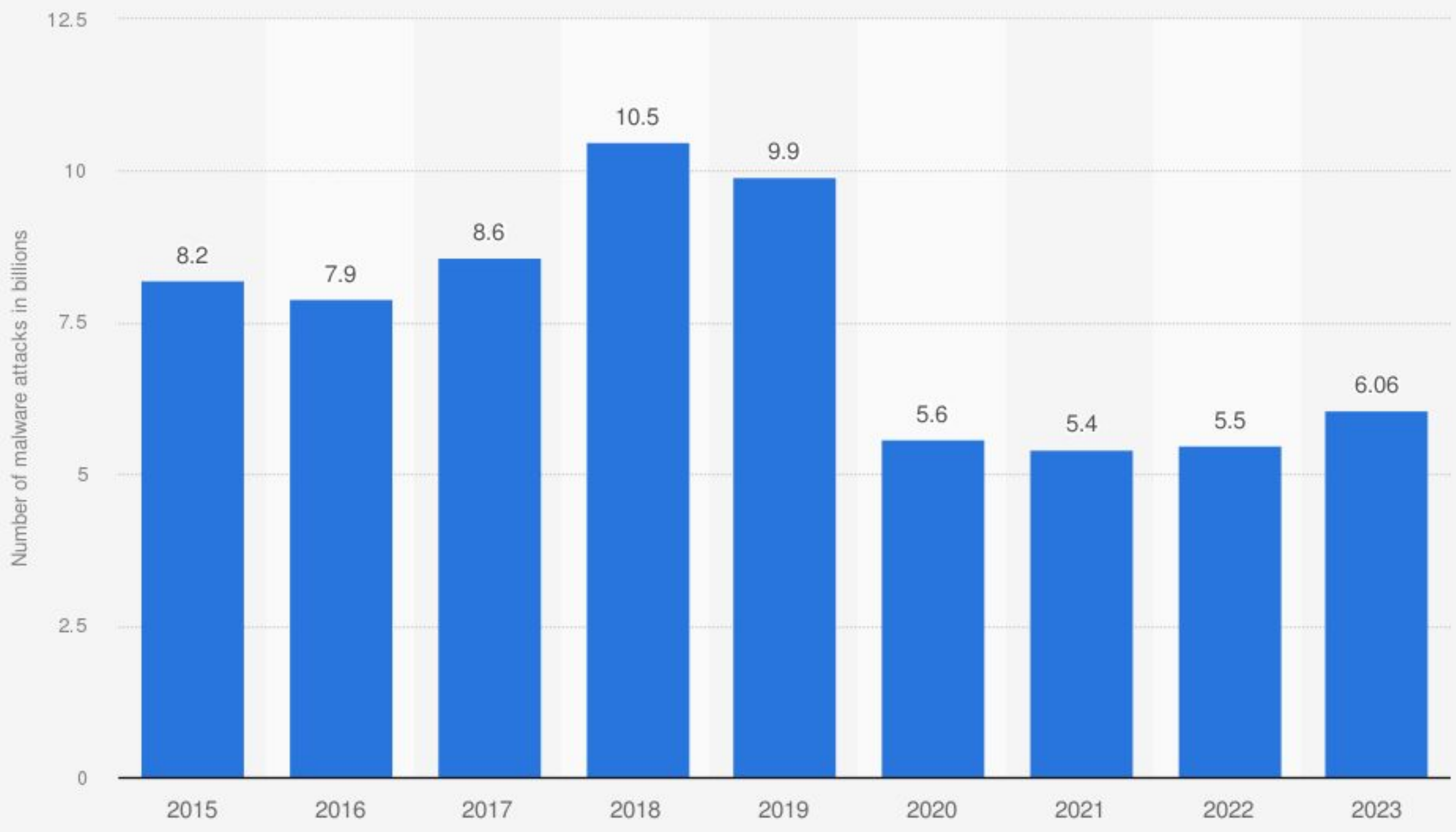
Image Credit
https://www.guardey.com/what-is-malware/

Why Does Malware Matter?

The threat landscape for malware is growing as a result of several evolving factors, making it an increasingly sophisticated and pervasive challenge for individuals, organizations, and governments.

Image Credit

Annual number of malware attacks worldwide from 2015 to 2023 (in billions)



Source
SonicWall
© Statista 2024

Additional Information:
Worldwide; SonicWall; 2015 to 2023; data is based on SonicWall Capture Labs characteristics; wider industry metrics may

Image Credit
https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/

Growth in Malware

Why is Malware continuing to grow?

1. Increased Attack Surface
   a. As more devices (smartphones, IoT devices, wearables) become connected, each device represents a possible vulnerability that can be exploited.
   b. The rise of remote work and the widespread adoption of cloud services, more sensitive data is stored and transmitted online. This shift has expanded the attack surface, making it easier for cybercriminals to target businesses and individuals from multiple vectors.

Image Credit

Growth in Malware (continued)

2. Sophistication of Attacks
    a. APTs (Advanced Persistent Threats) are highly targeted, long-term campaigns (usually) initiated by well-funded and organized groups (e.g., nation-states). These attacks are harder to detect, and the attackers stay hidden for extended periods to exfiltrate data or disrupt critical infrastructure.
    b. We have modern malware designed to change its code or appearance to evade detection by antivirus programs, such as polymorphic, metamorphic, and fileless.

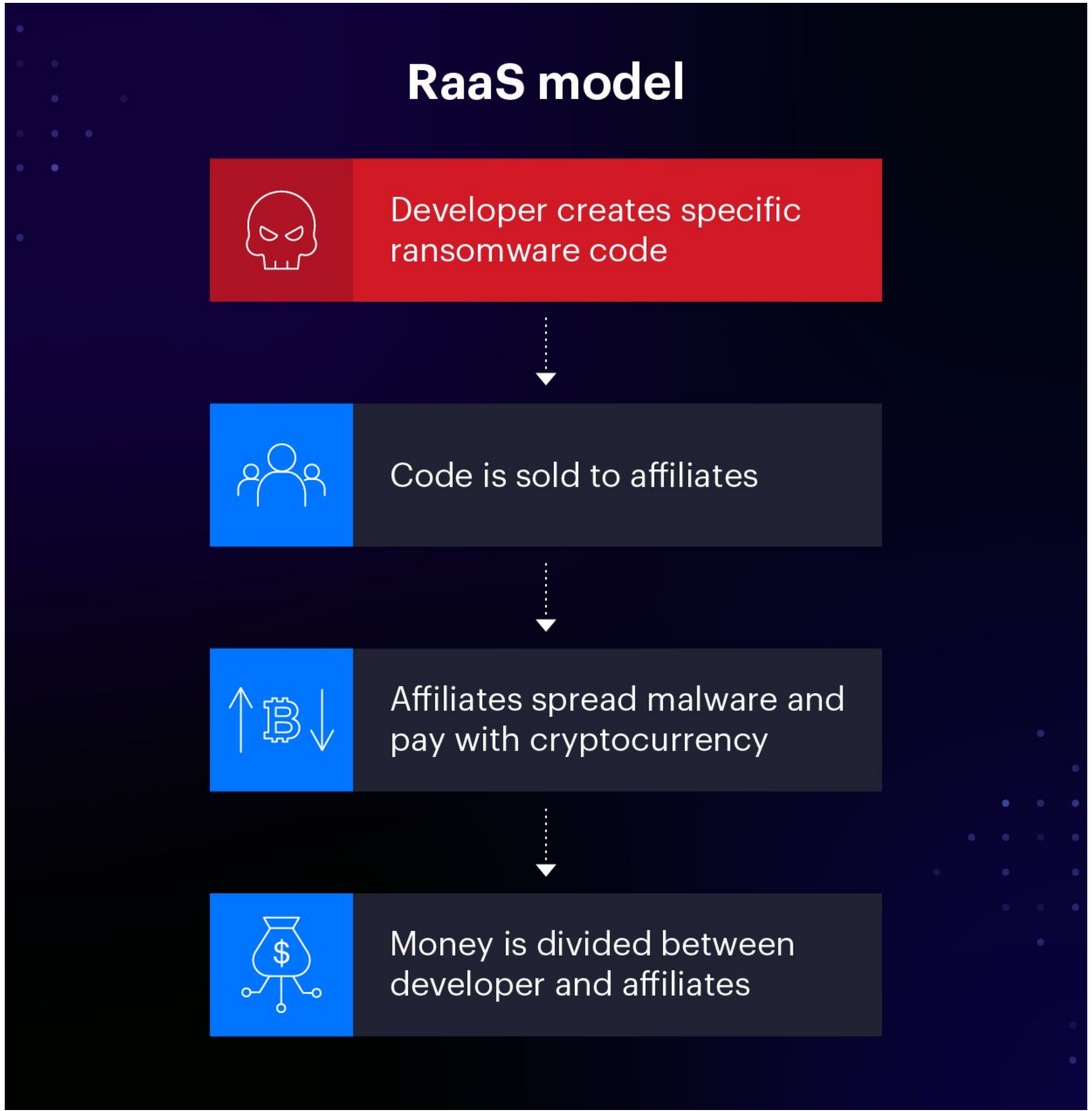
Image Credit

Growth in Malware (continued)

3. Ransomware Growth (Profit!)
   a. This has become one of the most prominent threats targeting critical infrastructure (healthcare, government, finance).
   b. Ransomware-as-a-Service (RaaS) has allowed even non-technical criminals to carry out attacks by “renting” out ransomware tools on the dark web.
   c. Also, attackers are increasingly employing double extortion tactics, where they not only encrypt data but also steal it and threaten to release it unless a ransom is paid.

<u>Why does Ransomware feel like a particularly difficult attack to stop?</u>

Image Credit



RaaS model

Developer creates specific ransomware code

Code is sold to affiliates

Affiliates spread malware and pay with cryptocurrency

Money is divided between developer and affiliates

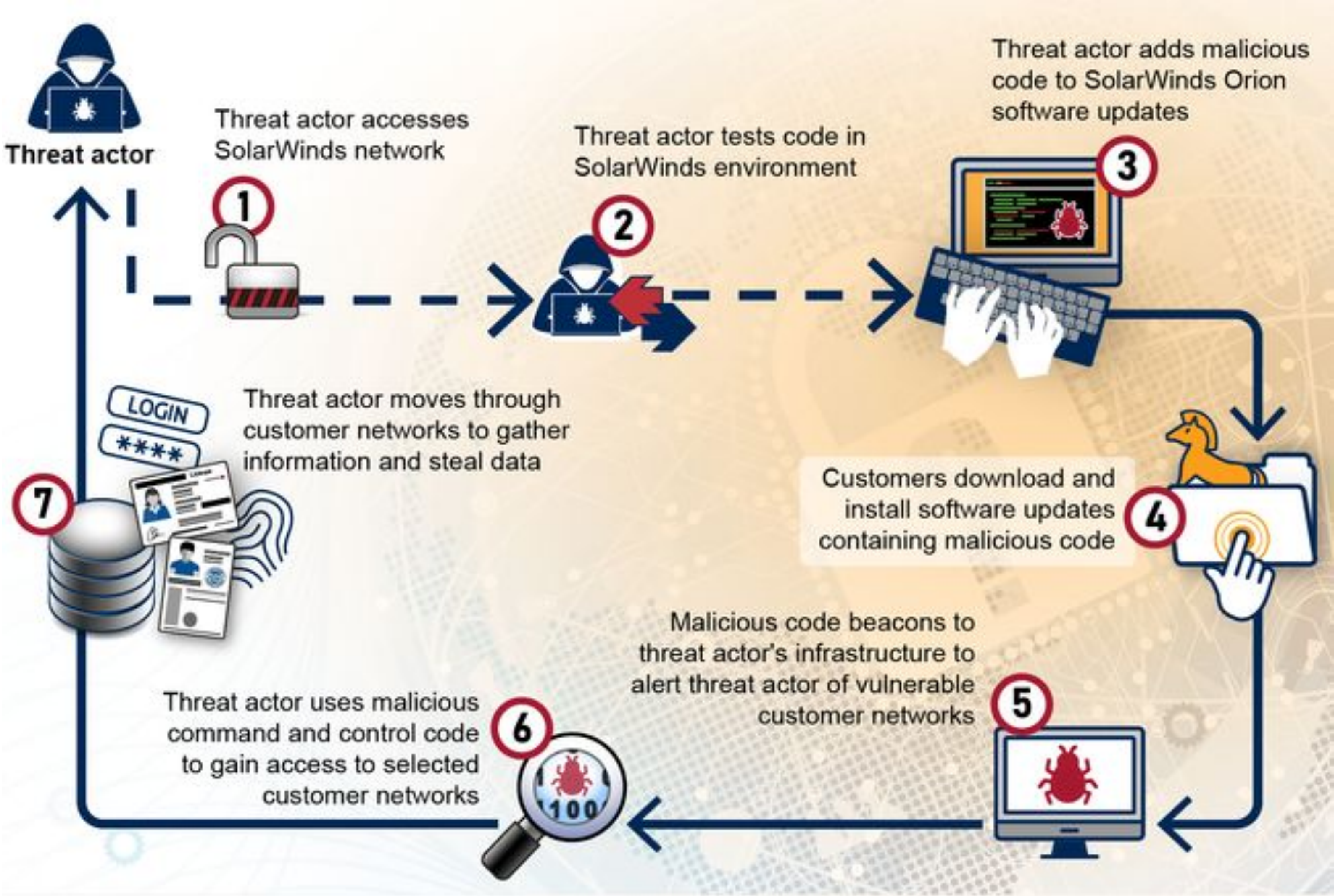
Image Credit
https://www.varonis.com/blog/ransomware-as-a-service

Growth in Malware (continued)

4. Targeting Critical Infrastructure
   1. There has been a rise in attacks against industrial control systems (ICS), such as power plants, water treatment facilities, and manufacturing plants. These systems can have severe real-world consequences, including physical damage and the loss of public services.
   2. The software supply chain is very susceptible, inserting malware into trusted software updates can allow attackers to infect multiple organizations through a single compromise.

Is anyone familiar with the SolarWinds attack?

Image Credit



1 Threat actor accesses SolarWinds network

2 Threat actor tests code in SolarWinds environment

3 Threat actor adds malicious code to SolarWinds Orion software updates

4 Customers download and install software updates containing malicious code

5 Malicious code beacons to threat actor's infrastructure to alert threat actor of vulnerable customer networks

6 Threat actor uses malicious command and control code to gain access to selected customer networks

7 Threat actor moves through customer networks to gather information and steal data

Source: GAO analysis of documentation from publicly released private industry and federal agency reports; images: kras99/stock.adobe.com, anna_leni/stock.adobe.com. | GAO-22-104746

Image Credit
https://www.gao.gov/products/gao-22-104746

Growth in Malware (continued)

5. Malware as a Service (MaaS)
   a. This is no longer the domain of **just** skilled hackers alone. You can now purchase or rent malware kits, exploit tools, and even attack services from underground markets (dark web).
   b. These malware-infected devices (botnets) can be rented out to carry out distributed denial-of-service (DDoS) attacks, spam campaigns, or other malicious activities.

Image Credit

Growth in Malware (continued)

6. Targeted Attacks on Individuals and Businesses
   a. The use of social engineering are becoming more sophisticated, and attackers impersonate trusted figures (such as colleagues, executives, or legitimate organizations) to trick individuals into clicking on malicious links or downloading infected attachments.
   b. This malware is then used to steal personal information, banking credentials, and sensitive business data. The attackers can then use stolen data for financial gain or sell it on the dark web (for more financial gain)..

Growth in Malware (continued)

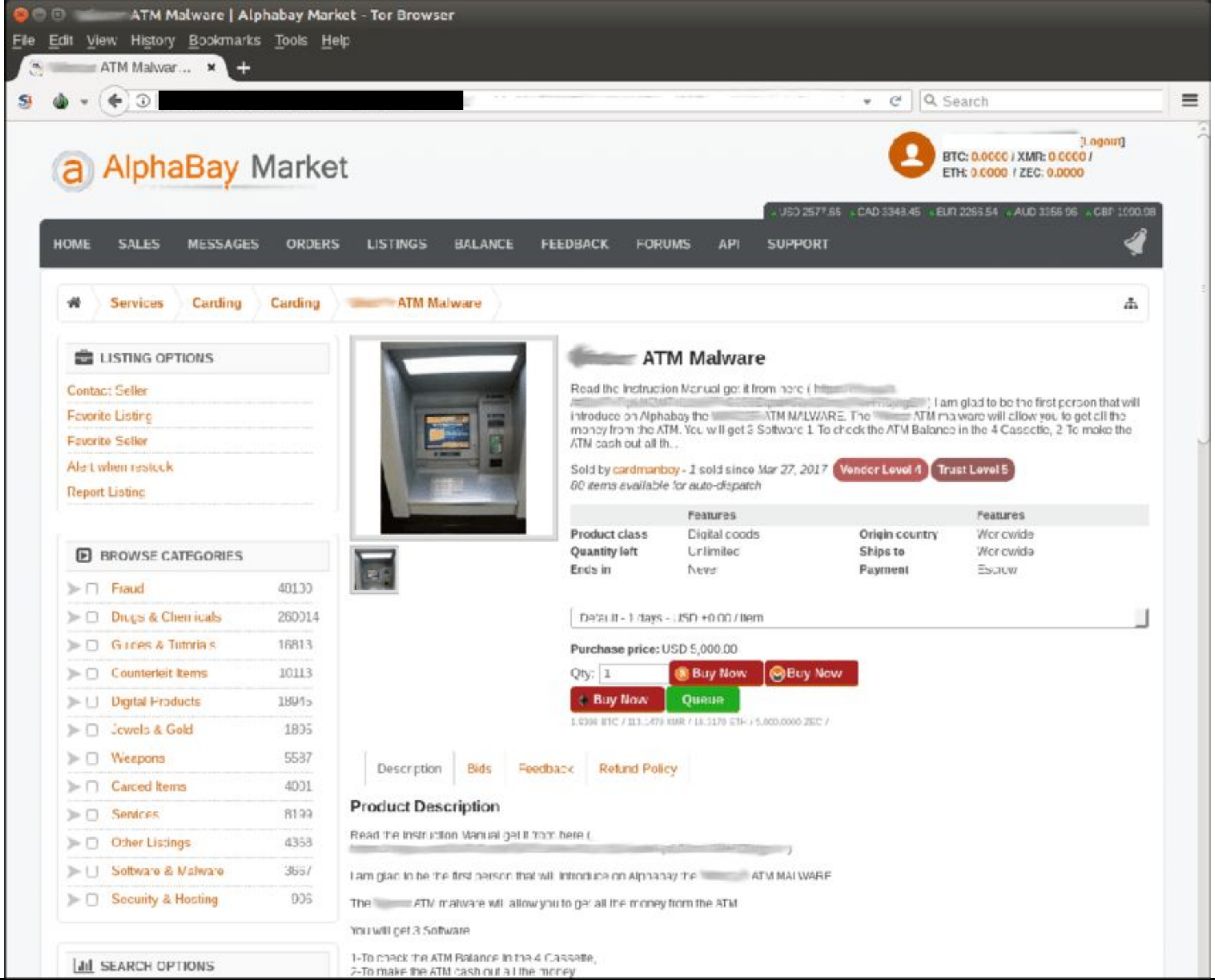
7. AI and Automation in Malware
    a. The use of AI and machine learning can help create more adaptive and efficient malware.
        i. The sample uses can include bypassing traditional security systems, optimize phishing attacks, and automate the spread of malware across large networks.
    b. AI tools can help automate the scan for vulnerabilities and launch attacks with little to no human intervention.

Image Credit

Growth in Malware (continued)

8. The Role of the Dark Web
   a. This hosts markets where malware, stolen data, and hacking tools are bought and sold.
   b. The users can access these resources without needing advanced technical knowledge.

Image Credit



BTC: 0.0000 / XMR: 0.0000 /
ETH: 0.0000 / ZEC: 0.0000

USD 2577.55 CAD 3348.45 EUR 2265.54 AUD 3356.06 GBP 1990.08

BROWSE CATEGORIES

□ Fraud	40130
□ Drugs & Chemicals	260014
□ Guides & Tutorials	16813
□ Counterfeit Items	10113
□ Digital Products	18945
□ Jewels & Gold	1895
□ Weapons	5537
□ Carded Items	4001
□ Services	8199
□ Other Listings	4358
□ Software & Malware	3657
□ Security & Hosting	906

ATM Malware

Read the Instruction Manual get it from here ([redacted]) I am glad to be the first person that will introduce on Alphabay the [redacted] ATM MALWARE. The [redacted] ATM malware will allow you to get all the money from the ATM. You will get 3 Software 1 To check the ATM Balance in the 4 Cassette, 2 To make the ATM cash out all th...

Sold by cardmanboy - *1 sold since Mar 27, 2017* Vendor Level 4 Trust Level 5
80 items available for auto-dispatch

	Features		Features
Product class	Digital goods	**Origin country**	Worldwide
Quantity left	Unlimited	**Ships to**	Worldwide
Ends in	Never	**Payment**	Escrow

Default - 1 days - USD +0.00 / item

Purchase price: USD 5,000.00

Qty: 1

1.9398 BTC / 113.1479 XMR / 18.2178 ETH / 5,000.0000 ZEC /

Product Description

Read the Instruction Manual get it from here ([redacted])

I am glad to be the first person that will introduce on Alphabay the [redacted] ATM MALWARE

The [redacted] ATM malware will allow you to get all the money from the ATM

You will get 3 Software

1-To check the ATM Balance in the 4 Cassette,
2-To make the ATM cash out all the money

Image Credit
https://hackread.com/you-can-now-buy-atm-malware-on-dark-web-for-5000/

Growth in Malware (continued)

9. Evolving Defenses and Challenges
    a. Traditional signature-based defenses, like antivirus software, are less effective against newer forms of malware (e.g., fileless, polymorphic, or zero-day attacks). To counter this, there is a growing shift toward behavioral analysis, machine learning, and AI-driven threat detection systems.
    b. Attackers are constantly searching for "zero-day" vulnerabilities (flaws in software that are unknown to the vendor) to exploit before patches can be released. Once discovered, these vulnerabilities can be exploited by malware until fixed.

Growth in Malware (continued)

10. Global and Geopolitical Considerations
    a. Nation-states are increasingly involved in cyber warfare, using malware to target the critical infrastructure and sensitive data of other nations.
    b. Governments are starting to put more focus on cybersecurity regulation, but these laws and frameworks are often struggling to keep pace with the rapid evolution of malware tactics.

Image Credit

Impact of Malware (2023 Statistics)

1. Every day, 560,000 new pieces of malware are detected.
2. There are now over 1 billion malware programs in existence.
3. Trojans account for 58% of all computer malware.
4. Every minute, four companies fall victim to ransomware attacks.
5. Android devices are 50 times more likely to be infected with malware than iOS devices.
6. Over the past decade, there has been an 87% increase in malware infections.
7. The cost of cybercrime is predicted to reach $8 trillion in 2023.
8. Open-source vulnerabilities are found in 84% of code bases

Is anyone starting to feel like cybersecurity is an impossible task? Why?

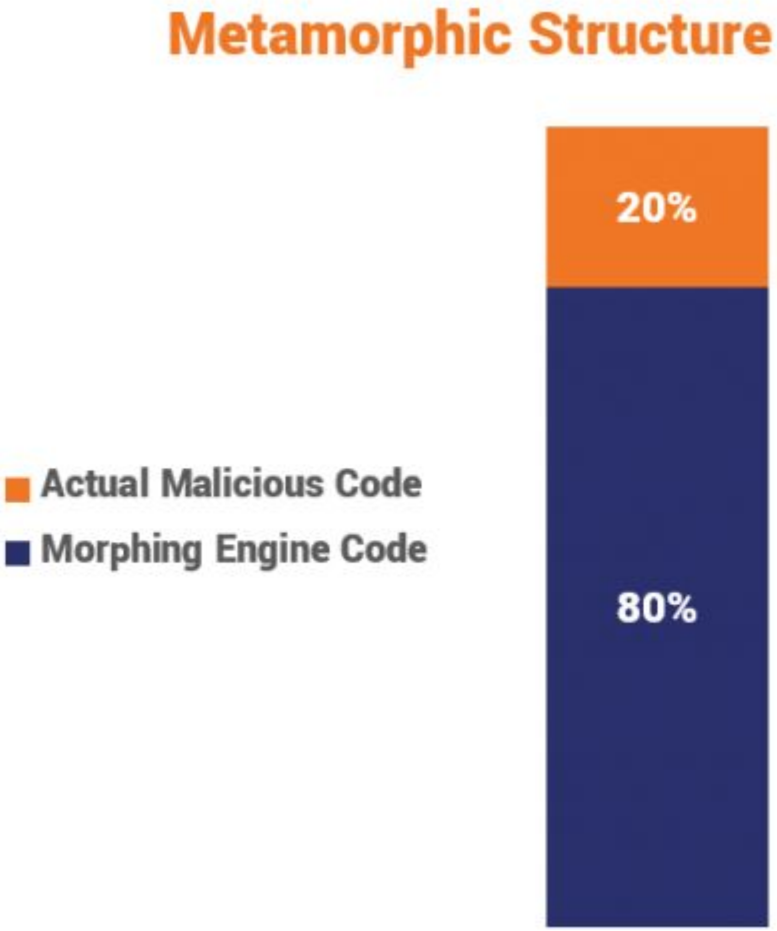
Image Credit

Malware Evolution

Polymorphic Malware: These change their code or structure each time they infect a new host to evade detection by antivirus software. The virus may alter its code using encryption or other methods.

Metamorphic Malware: These completely rewrite their own code each time they replicate. This makes them even harder to detect than polymorphic viruses.

Fileless Malware: A fileless malware operates within a computer's memory (RAM) rather than being stored as a file on the hard drive.



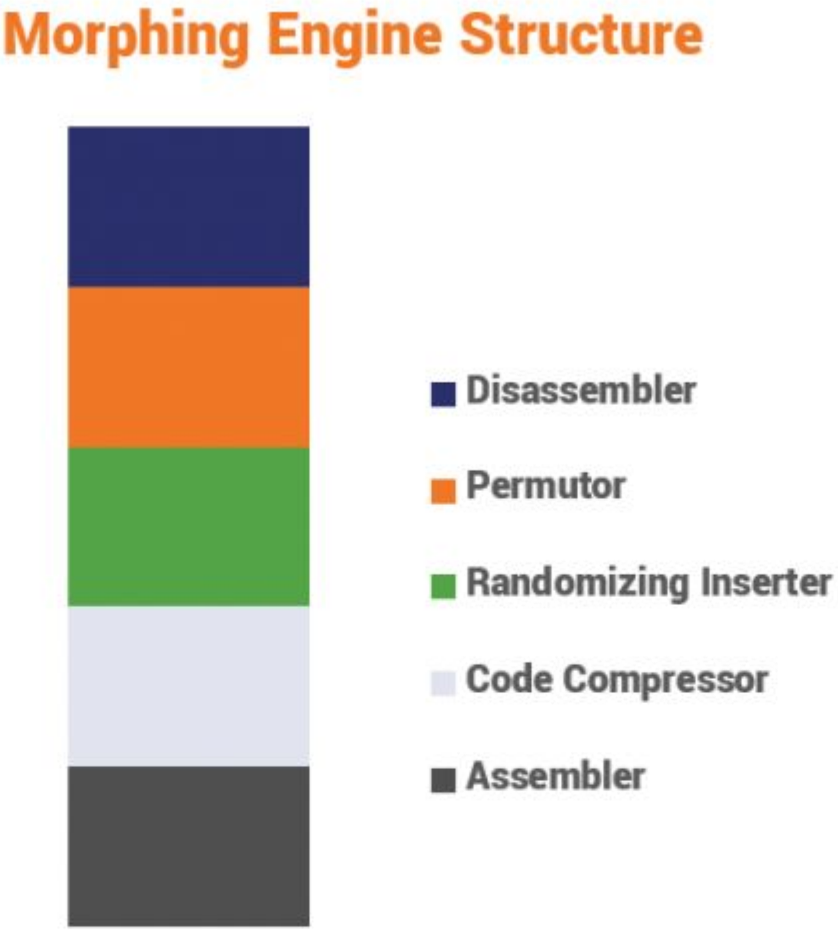


Image Credit
https://www.thesslstore.com/blog/polymorphic-malware-and-metamorphic-malware-what-you-need-to-know/

Virus

Virus

A virus, once executed, replicates itself and spreads to other programs, files, or systems, without the user's knowledge or consent.

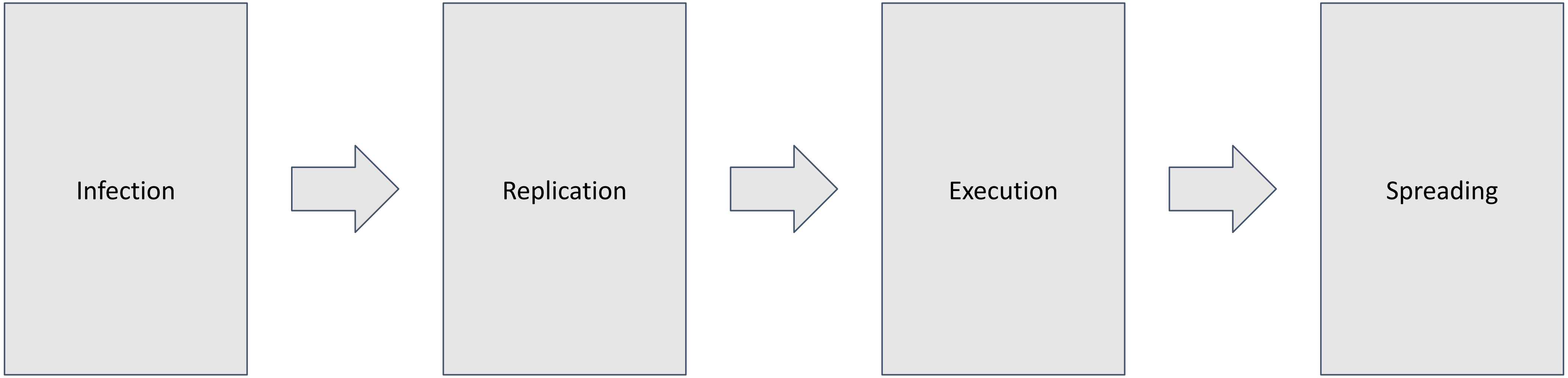


Image Credit

Virus (continued)

This is how a virus works:

1. Infection - The virus (typically) requires a host program or file to attach itself to in order to spread. This is how the virus begins its life cycle, and can do this in a couple of ways:
    a. Host Selection: The virus targets executable files, scripts, or documents that are commonly opened by users (e.g., `.exe`, macros in `.docx` or `.xls` documents, or script files like `.bat` or `.vbs`).
    b. Code Injection: Once the virus identifies a target file, it injects its own malicious code into the target. The virus may append its code to the end of the host file or embed it within the file itself (in the case of document-based viruses, like macro viruses).

Image Credit

Virus (continued)

2. Replication - The defining characteristic of a virus is its ability to replicate and spread to other systems or files.
   a. Self-Replication: The virus is designed to copy itself into new files, applications, or even system components. It does this by modifying the code of other programs or creating new files that contain a copy of its own code. This is often done automatically without the need for human intervention.
   b. Trigger Mechanism: Some viruses use a trigger that activates them under certain conditions (e.g., a specific date, a user action, or a particular system event). This is where the virus switches from simply hiding and waiting to actively causing damage or further spreading.

Virus (continued)

3. Execution - The virus waits for an opportunity to execute its payload. This happens when the infected triggers are met.
   a. Payload: The payload is the malicious part of the virus. It could range from benign actions, like annoying pop-ups, to severe actions like deleting files, corrupting data, stealing sensitive information (e.g., keystrokes or passwords), or opening backdoors to allow remote access.

Virus (continued)

4. Spreading - After successfully infecting one system, the virus attempts to propagate further, spreading its infection to other computers or networks.
   a. Email Attachment: One common way for a virus to spread is by attaching itself to email messages.
   b. Removable Media: They can propagate via USB drives or external hard drives. When the infected device is connected to another computer, the virus copies itself onto that machine.
   c. Network Propagation: In some cases, viruses are designed to exploit vulnerabilities in a computer network to propagate themselves.
   d. Social Engineering: Some viruses exploit social engineering techniques, tricking users into running infected files or clicking on malicious links.

Image Credit

Virus Types

1. File Deletion: These delete files or folders on the infected system, causing data loss.
2. Data Corruption: The viruses corrupt files, making them unusable or altering their content.
3. Keylogging: These are designed to log keystrokes and capture sensitive information, such as passwords or credit card numbers.
4. Denial-of-Service (DoS): These can use the machine to launch a DoS attack by overwhelming a server with traffic, causing it to become unresponsive.
5. Backdoor Installation: This creates backdoors (hidden entry points) that allow attackers to gain remote access to the infected system.
6. Ransomware Payloads: They act as ransomware, encrypting files on the victim's system and demanding a ransom for their decryption.

Image Credit

Worm

Worm

A computer worm is a type of self-replicating malware designed to spread across computers and networks without requiring any human intervention.

Image Credit
https://www.emsisoft.com/en/blog/28154/computer-worms/

Worm (continued)

The worm is capable of making copies of itself. Once it infects a system, it can create additional copies that can spread to other systems.

The distinction between a worm and a virus is that typically a virus requires a user to execute an infected file or program. The worm can spread automatically.

Image Credit

Worm (continued)

This is how a worm works:

1. The worm will look for security flaws in software or operating systems.
2. It will often scan other machines on the same network or over the internet. It tries to find machines that are vulnerable to the same exploit it used to infect the initial machine.
    a. The worms also spread through email, embedding themselves in attachments or the body of the email, which they then send out to contacts in the infected system's address book.
    b. A worm can also spread by attaching itself to downloadable files on file-sharing networks or websites, and once downloaded by a user, it can start spreading further.

Image Credit

Worm Types

Network congestion: The worms replicate and send themselves to other computers, they can generate a lot of network traffic, which can slow down or even crash networks.

Resource consumption: The worm consumes system resources, such as CPU and memory, by constantly replicating itself, which can degrade system performance.

Denial of Service (DoS): They can be used to flood a network with traffic, preventing legitimate users from accessing the system or network.

Image Credit

Trojan

Trojan

Does anyone know the Greek story of the Trojan Horse?

Image Credit

Trojan

Does anyone know the Greek story of the Trojan Horse?

A Trojan (horse) malware attack is a type of cyber attack where malicious software is disguised as legitimate or benign software to trick users into installing or executing it.

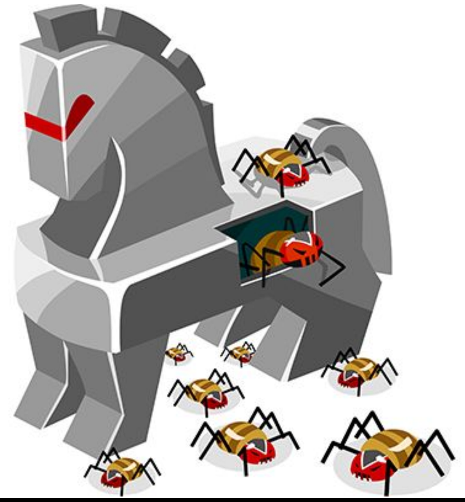


Image Credit
https://enterprise.xcitium.com/wp-content/uploads/2022/10/what-is-a-computer-trojan-1.png

Trojan (continued)

This is how a trojan works:

1. The attacker uses deception to convince the user to download or execute the Trojan.
    a. This can be in the form of an email attachment, a fake software update, or a compromised file on a website.
    b. The Trojan may appear to be a useful application, such as a game, a software update, or a system utility, which makes the user more likely to run it.
2. Once the Trojan is installed or executed, it delivers the payload and typically runs in the background of the system, often without alerting the user to its presence.

Image Credit

Trojan Types

1. “Backdoor” Trojan - This opens a "backdoor" to allow remote access to the infected machine.
2. Downloader Trojan - Downloads and installs additional malware after the Trojan is executed.
3. Infostealer Trojan - The focus is on stealing sensitive information, such as login credentials, financial data, or personal information.
4. RAT (Remote Access Trojan) - This provides remote access to attackers, allowing them to control the system and perform actions.
5. Banking Trojan - These can be specifically designed to steal banking credentials and other financial information.

Image Credit

Spyware

Spyware

A type of malware designed to secretly monitor or collect information about a user's activities without their knowledge or consent.

It can compromise the confidentiality, integrity, and privacy of a system, and may transmit sensitive information back to an attacker or third party.

Image Credit

Spyware (continued)

This is how spyware works:

1. Installation - Spyware can be installed on a victim's device through various means we have already covered.
   a. Bundling: Spyware is often bundled with seemingly legitimate software, which is installed unintentionally when the user installs the primary application.
2. Persistence: It will use techniques to remain persistent on the system, even after a reboot or attempts to remove it. This might involve modifying system files or adding itself to startup processes.
3. Communication: They can communicate with external servers to send collected data back to the attacker. This could happen through HTTP/HTTPS requests, encrypted tunnels, or other covert communication protocols.

Image Credit

Spyware Types

Data Collection: This is primarily used to monitor and gather data from the infected system. This can include browsing history, login credentials, personal information, financial data, email content, keystrokes, and other sensitive data.

Tracking and Surveillance: It can track user activity, such as website visits, application usage, and even physical locations through GPS or IP tracking.

Credential Theft: This spyware may specifically aim to capture sensitive credentials (e.g., usernames and passwords) entered into websites, applications, or databases.

Adware

Adware

Adware is a type of software that automatically displays or downloads unwanted advertisements on your computer. It can be bundled with free software or downloaded from dubious websites.

*While adware itself isn’t typically malicious, it can slow down your computer, affect your browsing experience, and even compromise privacy in some cases.

Image Credit

Adware (continued)

Here is how adware works:

1. Installation: Often, adware is installed unintentionally when you download and install free software, especially from less trustworthy sites. It might be included as an optional add-on that the user doesn't notice during installation.
2. Display Ads: Once installed, the adware starts to display ads on your computer. These ads can appear as pop-ups, banners, or even in your web browser. They might be related to your browsing activity or could be random.

Image Credit

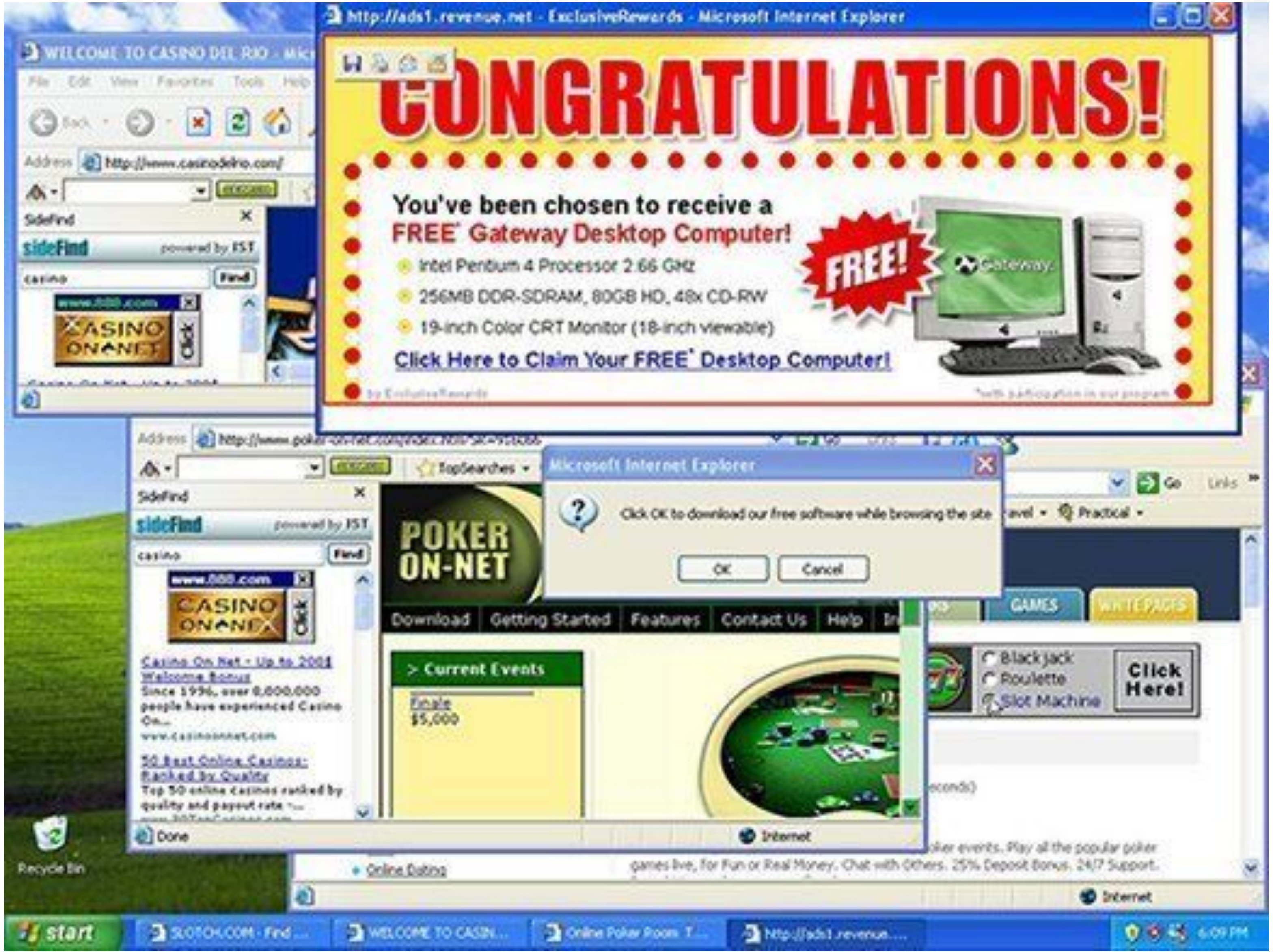
Adware (continued)

These are some other notes about Adware:

- It can sometimes collects information about your browsing habits, search history, and online activities to show you targeted ads. It often does this to increase the effectiveness of its ads and generate more revenue for the creators of the adware.

- Redirecting Web Traffic: In some cases, adware may redirect you to certain websites that are meant to generate revenue through ad views or clicks.

Image Credit



http://ads1.revenue.net - ExclusiveRewards - Microsoft Internet Explorer

CONGRATULATIONS!

You've been chosen to receive a FREE* Gateway Desktop Computer!

- Intel Pentium 4 Processor 2.66 GHz
- 256MB DDR-SDRAM, 80GB HD, 48x CD-RW
- 19-inch Color CRT Monitor (18-inch viewable)

Click Here to Claim Your FREE* Desktop Computer!

*with participation in our program

Microsoft Internet Explorer

Click OK to download our free software while browsing the site

OK Cancel

Casino On Net - Up to 200$ Welcome Bonus
Since 1996, over 8,000,000 people have experienced Casino On...
www.casinoonnet.com

50 Best Online Casinos: Ranked by Quality
Top 50 online casinos ranked by quality and payout rate -...

Image Credit
https://www.techtarget.com/rms/onlineImages/security-adware_mobile.jpg

Rootkits

Rootkit

A rootkit is a type of malware designed to gain unauthorized access to a computer system and maintain control without being detected.

A rootkit's primary goal is to gain privileged access (root access, get it?) to a computer system and conceal its presence and other harmful activities

Image Credit

Rootkit (continued)

This is a how a rootkit works:

1. Installation - Rootkits typically enter the system via social engineering, phishing, vulnerabilities in software, or exploitation of unpatched system flaws.
   a. **This should be starting to feel very familiar to our other malware…**
2. Escalating Privileges - This attempts to escalate its privileges to root This ensures it has full control over the system.
3. Persistence and Concealment - The rootkit attempt to maintain their presence and avoid detection by hiding files, processes, or registry entries that might expose their activity.

Image Credit

Rootkit Types

User-mode Rootkits: These operate at the application level and manipulate or hook system processes and API calls to intercept user actions or hide malicious behavior. They typically target high-level system processes and are less sophisticated.

Kernel-mode Rootkits: These run at the kernel level and have full access to the system’s core functionality.

- They can intercept system calls and modify core OS components like the kernel, device drivers, and file systems to remain hidden. Kernel-mode rootkits are much harder to detect and remove.

Image Credit

Rootkit Types (continued)

Bootkits: A rootkits that infects the boot process, usually by modifying the Master Boot Record (MBR) or the system’s UEFI/BIOS. Bootkits load **before the operating system**, making them difficult to detect by traditional security software, as they can compromise the system even before the OS starts.

Firmware Rootkits: These target the firmware of a system (e.g., BIOS/UEFI) or peripherals (e.g., network cards or hard drives). Since firmware is often outside the control of OS-level security software, detecting these rootkits requires specialized tools.

Image Credit

Protecting Against Malware

Protecting Against Malware

I know that was a lot, thank you for continuing to follow along (or at least pretending to).

We can take a couple minutes to chat with the people around you, and think about:

What are some ways we can protect against malware? It is okay if you don't know all the technical strategies, you can focus on the human-aspect!

Protecting Against Malware (continued)

Educating Users and Raising Awareness

- The first and most important line of defense is user awareness. Many malware infections are caused by user mistakes, such as clicking on malicious links, downloading infected attachments, or visiting malicious websites.

Regular Software Updates and Patch Management

- Malware often exploits vulnerabilities in outdated software or unpatched systems. Keeping software up-to-date is one of the most effective defenses against malware.

Image Credit

Protecting Against Malware (continued)

Antivirus and Anti-Malware Software

- Using **reputable** antivirus and anti-malware software is essential for identifying and removing malware from the system. These tools use signature-based detection, heuristic analysis, and behavioral detection to find malicious software.

Firewalls (Network and Host-based)

- A firewall serves as a barrier between trusted internal networks and potentially dangerous external networks (e.g., the internet). It monitors incoming and outgoing network traffic to detect and block malicious activity.

Image Credit

Protecting Against Malware (continued)

Use of Sandboxing and Virtualization

- Sandboxing and virtualization are advanced techniques to isolate potentially dangerous applications or unknown files from the rest of the system.

Application Whitelisting

- Application whitelisting is the practice of only allowing approved and known-good applications to run on the system, blocking everything else.

Image Credit

Protecting Against Malware (continued)

Network Segmentation and Isolation

- If malware does manage to infiltrate the network, network segmentation can help limit its spread.

Behavioral and Heuristic Detection

- Malware signatures can change over time, making it harder for traditional signature-based detection methods to identify new threats. Behavioral analysis and heuristic techniques can help detect malware based on its actions, even if its signature is unknown.

Image Credit

Protecting Against Malware (continued)

Backup and Recovery Plans

- Having robust backup and disaster recovery plans in place ensures that data can be restored in the event of a malware attack (especially ransomware).

Least Privilege and Access Control

- Implement the principle of least privilege (PoLP) by limiting users' access to only the resources necessary for them to perform their job functions. This minimizes the damage that malware can cause if a user’s account is compromised.

Protecting Against Malware (continued)

Incident Response and Forensics

- Prepare for the worst by having an incident response plan in place. Knowing how to respond quickly to a malware infection can minimize its impact.

Image Credit

Discussion Questions (groups)

Should individuals or organizations be held responsible for malware infections caused by not following basic cybersecurity hygiene (e.g., neglecting software updates, using weak passwords)? Why or why not?

We have discussed patches and the role they play in cybersecurity. Do you think patches can be your main defense strategy against attacks?

Discuss the legal challenges in prosecuting cybercriminals who create and distribute malware. What international cooperation efforts are needed to combat these threats effectively?

Image Credit

Questions?

References

[1] https://www.getastra.com/blog/security-audit/malware-statistics/#:~:text=Android%20devices%20are%2050%20times,reach%20%248%20trillion%20in%202023.