
OnlyMalware

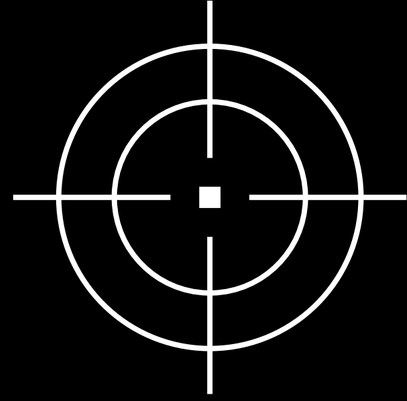
Moving Target Defense (MTD) to Combat Advance Persistent Threats (APTs) and In-Memory Malware

~$ whoami

- Researcher at Indian Institute of Technology Bombay (IIT-B)
- Worked with National Critical Information Infrastructure Protection Center (NCIIPC), a unit of the National Technical Research Organization (NTRO) as Cybersecurity Intern.
- M.S.c in Cyber Security & Digital Forensics , Bachelors of Computer Applications (BCA)
- Winner of national level hackthon “Cython 2024” which was conducted by IIT-D & NCIIPC
- FOSS enthusiast

Agenda

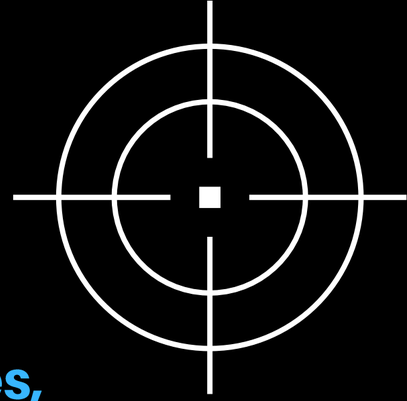
- Introduction to Moving Target Defense (MTD).
- Application of MTD to counter Advanced Persistent Threats (APTs).
- Future potential and application of MTD to counter advanced in-memory malware.



Moving Target Defense (MTD)

BEFORE MOVING AHEAD LETS PLAY A SMALL GAME

Static IT Systems

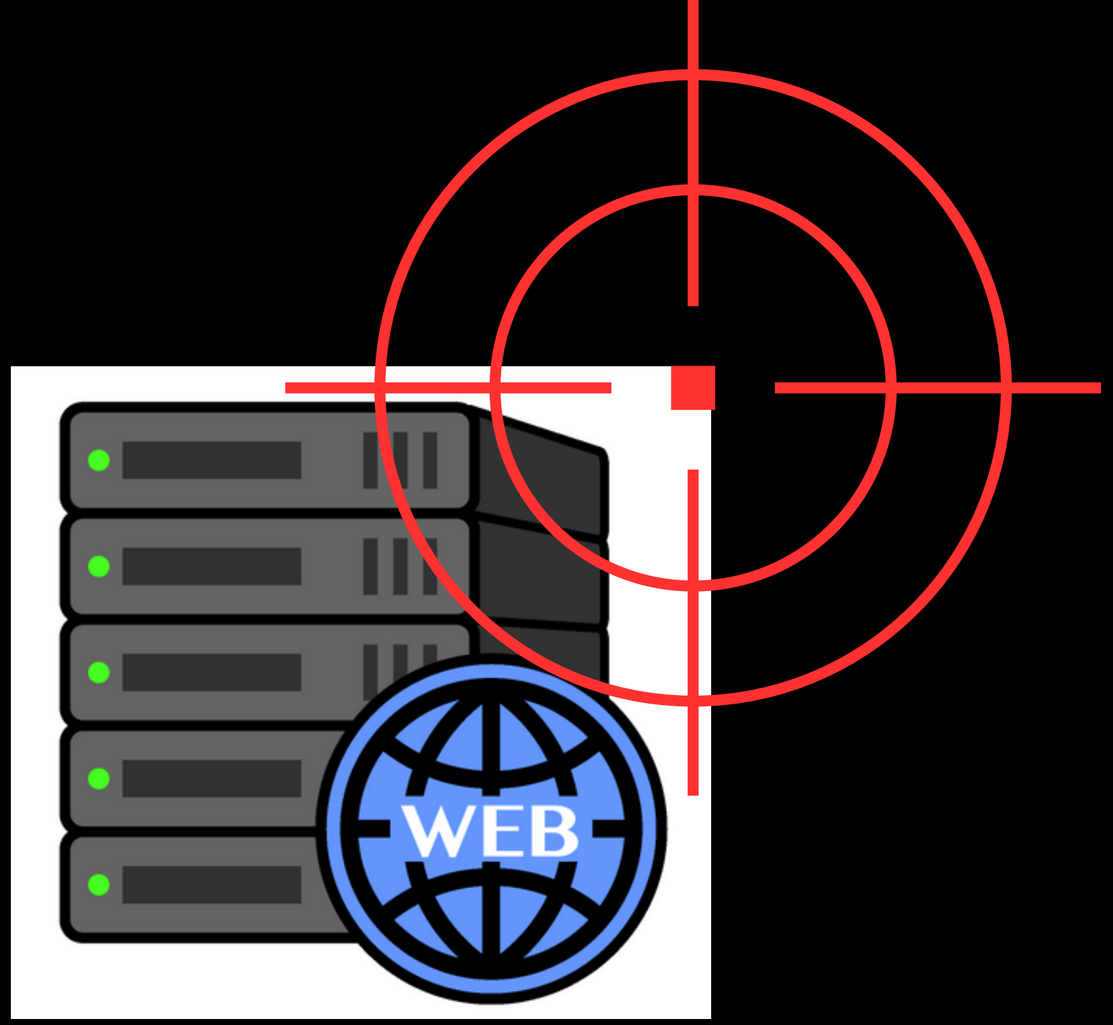


- Traditional IT systems are designed with static configurations (e.g., addresses, software stacks, networks).
- These systems were built for simplicity, with configurations remaining unchanged over time.
- Static configurations give attackers time to plan and execute attacks with ease.

Moving Target Defense（MTD）

- Dynamic Cybersecurity Strategy: Constantly changes the attack surface to protect systems and data.
- Increase Uncertainty for Attackers: Adds complexity, reducing their window of opportunity.
- Higher Attack Costs: More resource-intensive.

CONSIDER A WEB SERVER



TARGET OF CYBER ATTACK

- If MTD keeps dynamically changing the IP address of the server, the attackers have to deal with the dynamic IP address changes while accessing the server to attack.
- Attacker will require extra time and effort for a successful attack, and the probability of success will be small.
- Thus, using MTD, attackers must deal with dynamic changes when attacking these targets, making it more difficult to attack them.

NOTE ⚠

MTD DOES NOT FIX THE VULNERABILITY ITSELF, IT CAN MAKE CYBER-ATTACKS MORE DIFFICULT THROUGH CHANGING SYSTEM MODIFICATIONS DYNAMICALLY, BECAUSE IT REDUCES THE PROBABILITY OF SUCCESS AND INCREASES THE TIME UNTIL SUCCESSFUL ATTACKS.

SO IT CAN BE AN EFFECTIVE METHOD AGAINST ZERO-DAY ATTACKS.

MTD Techniques:

1. Dynamic Data: Alters format, syntax, encoding, or data representation dynamically.
2. Dynamic Software: Changes application code, instructions, and format in real-time.
3. Dynamic Runtime Environment: Modifies execution environment, including address space and instruction set randomization.
4. Dynamic Platforms: Techniques that dynamically change platform properties, eg., OS, CPU architecture
5. Dynamic Networks: Adjusts network properties (e.g., IP address, port number, routing) dynamically.

MTD APPLICATIONS EXTEND ACROSS AREAS SUCH AS DEEP LEARNING, POWER SYSTEMS, AND IOT.

https://apps.dtic.mil/sti/pdfs/AD1055276.pdf

Moving Target Defense (MTD) to counter Advance Persistent threat (APTs)

Advance persistent threats (APTs)?

SideCopy APT Targets India's Premier Defense Research Agency

SideCopy APT Used Decoy Documents in Spear-Phishing Attack on DRDO

Jayant Chakravarti (@JayJay_Tech) · March 23, 2023

Share Tweet Share Credit Eligible Get Permiss

BlackBerry Cybersecurity Automotive & IOT Critical Communications

Transparent Tribe Targets Indian Government, Defense, and Aerospace Sectors Leveraging Cross-Platform Programming Languages

RESEARCH & INTELLIGENCE / 05.22.24 / The BlackBerry Research and Intelligence Team

ADVANCED PERSISTENT THREAT

Transparent Tribe (APT36) | Pakistan-Aligned Threat Actor Expands Interest in Indian Education Sector

ALEKSANDAR MILENKOSKI / APRIL 13, 2023

SideCopy APT group uses ReverseRAT backdoor to target Indian government agencies, ThreatMon reports

FEBRUARY 21, 2023

कौन? क्या?

क्या?

- Nation-state supported hackers
- Generally more sophisticated
- Lot of resources & funding

क्या?

- Nation-state supported hackers
- Generally more sophisticated
- Lot of resources & funding

ADVANCED

- (Special) malware

क्या?

- Nation-state supported hackers
- Generally more sophisticated
- Lot of resources & funding

ADVANCED

- (Special) malware
- Special operations & operators.

क्या?

- Nation-state supported hackers
- Generally more sophisticated
- Lot of resources & funding

ADVANCED

- (Special) malware
- Special operations & operators.

PERSISTENCE

- Long term presence

क्या?

- Nation-state supported hackers
- Generally more sophisticated
- Lot of resources & funding

ADVANCED

- (Special) malware
- Special operations & operators.

PERSISTENCE

- Long term presence
- Multi step

क्या?

- Nation-state supported hackers
- Generally more sophisticated
- Lot of resources & funding

ADVANCED

- (Special) malware
- Special operations & operators.

PERSISTENCE

- Long term presence
- Multi step
- Low & slow

क्या?

- Nation-state supported hackers
- Generally more sophisticated
- Lot of resources & funding

ADVANCED

- (Special) malware
- Special operations & operators.

PERSISTENCE

- Long term presence
- Multi step
- Low & slow

THREAT

- Targeted at high value organization & information


KON HAI YE LOG?
KAHA SE AATE HAI YE LOG?

PANDAS

Meet “Pandas”

APT Name	Active Since	Tactics, Techniques, Procedures	Targets
Comment Panda (AKA APT1, Comment Crew)	2006	Spear phishing, custom backdoors	IT, Aerospace, Public Administration, Satellites, Telecom, Scientific Research, Energy, Transportation, Manufacturing, Engineering, Electronics, International Organizations, Advertising and Entertainment, Navigation, Chemical, Financial, Healthcare, Education
Stone Panda (AKA APT10, Cicada, menuPass)	2009	Spear phishing, managed service providers	Construction and Engineering, Aerospace, Telecom, Government
Kryptonite Panda (AKA APT40, Gadolinium, Leviathan)	2009	Spear phishing	Engineering, Defense
Emissary Panda (AKA APT27, BRONZE UNION, LuckyMouse)	2010	Spear phishing, zero-day exploits	Government, Energy, Aerospace, Transportation, Travel, Technology
Wicked Panda (AKA APT41, Winnti, Group 72, Barium, Lead)	2012	Often changes, custom malware, exploitation of zero-day and unpatched vulnerabilities	Academic, Manufacturing, Telecom, Technology, Agriculture, Industrials, Engineering, Hospitality, Think Tanks, Chemical

KITTENS

Meet “Kittens”

APT Name	Active Since	Tactics, Techniques, Procedures	Targets
Refined Kitten (AKA APT33, Elfin)	2013	Spear phishing, brute force, password spraying, domain masquerading	Aviation, energy, petrochemical
Rampant Kitten	2014	Infostealer malware, ransomware	Government, Technology, Defense
Rocket Kitten (AKA Newscaster, Phosphorus, Charming Kitten, Saffron Rose)	2010	Social engineering, social media phishing, spear phishing, Microsoft Office vulnerabilities	Military, Government, Media, Energy, Defense Industrial Base, Engineering, Telecom, dissidents
Helix Kitten (AKA APT34, OilRig, GreenBug, IRN2)	2014	Spear phishing, social engineering (LinkedIn), DNS tunneling, Microsoft Office vulnerabilities	Aerospace, Energy, Financial, Government, Hospitality, Telecom
Remix Kitten (AKA Chafer, Cadelle, APT39, ITG07)	2014	Spear phishing, social engineering, SQL injection, custom backdoors	Aviation, Telecom, Technology, Hospitality, Travel
Pioneer Kitten (AKA Fox Kitten, PARISITE, UNC757)	2017	Exploiting unpatched vulnerabilities, web shells	Healthcare, Government, Technology, Defense
Static Kitten (AKA MuddyWater, Seedworm)	2017	Spear phishing, Powershell Trojans	Government, Tourism, Telecom

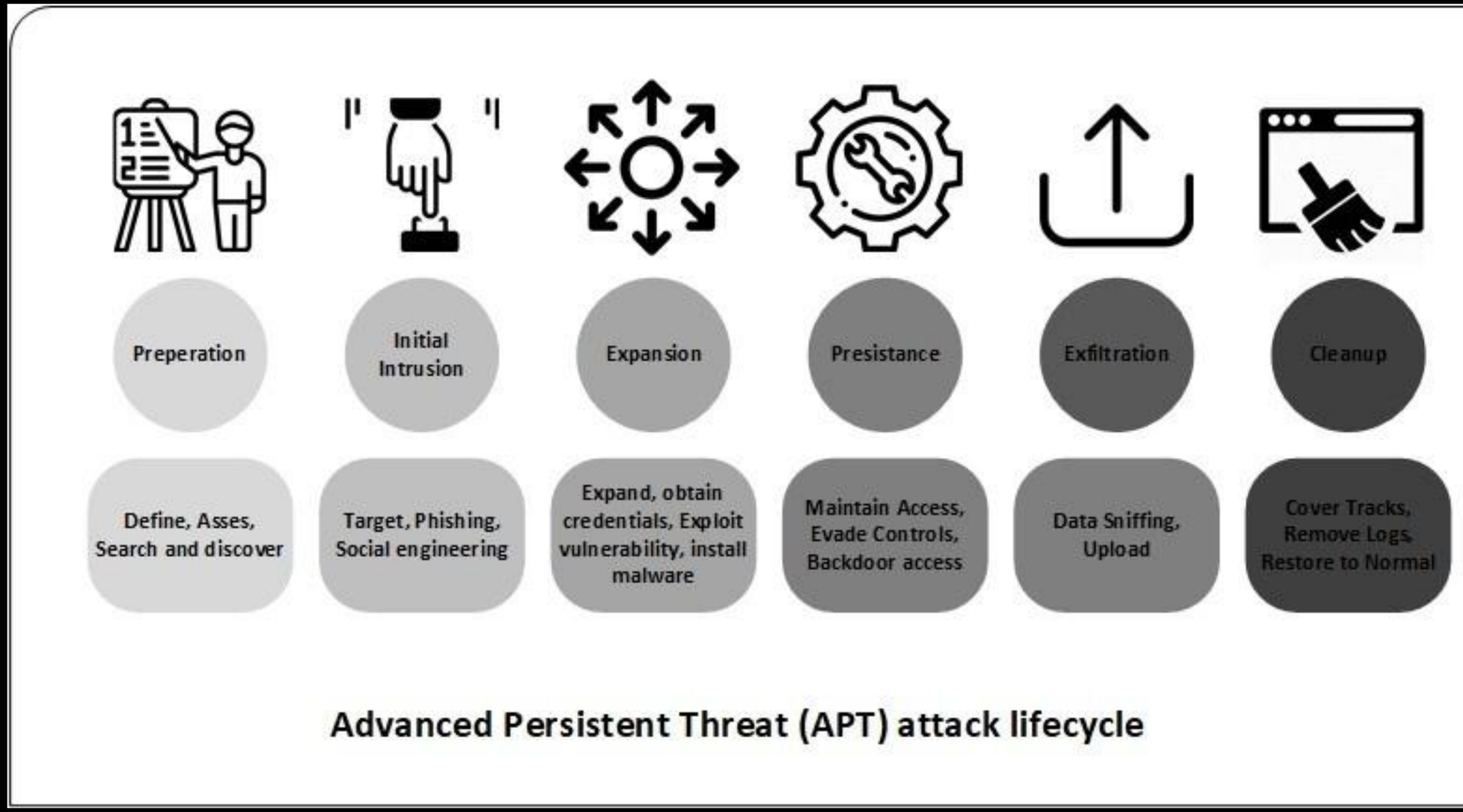
BEAR

Meet “Bears”

APT Name	Active Since	Tactics, Techniques, Procedures	Targets
Fancy Bear (AKA APT28, Zebrocy, Sofacy)	2004	Password spraying, brute force attacks, spear phishing, drive-by web compromise, exploit public-facing application vulnerabilities, SQL injection, denial-of-service attacks, weaponized Office documents	Energy, Government, Media, Aerospace, Military, NGOs, Nonprofits, Hospitality, Political Parties
Cozy Bear (AKA APT29, The Dukes)	2008	Spear phishing, password spraying, steganography, exploit public-facing application vulnerabilities	Academic, Energy, Financial Services, Government, Media, Technology, Aerospace, Industrials, Engineering, NGOs, Nonprofits, Pharmaceuticals, Oil and Gas, Insurance
Venomous Bear (AKA Turla, Uroboros)	2004	Spear phishing, watering hole attacks, use of sophisticated custom malware	Academic, Government, Telecom, Aerospace, NGOs, Nonprofits, Defense

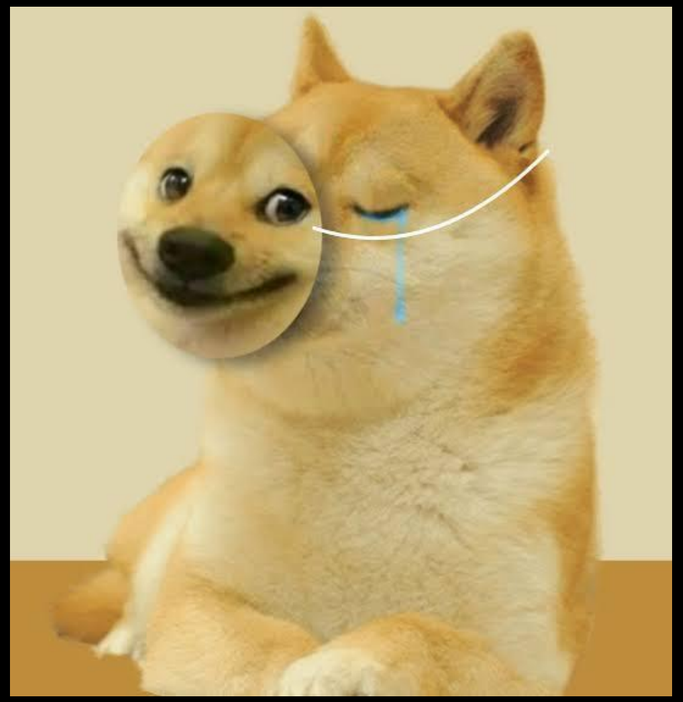
- It’s a broad term used to describe an attack campaign in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network in order to mine highly sensitive data.
- The goal of most APT attacks is to achieve and maintain ongoing access to the targeted network rather than to get in and out as quickly as possible.

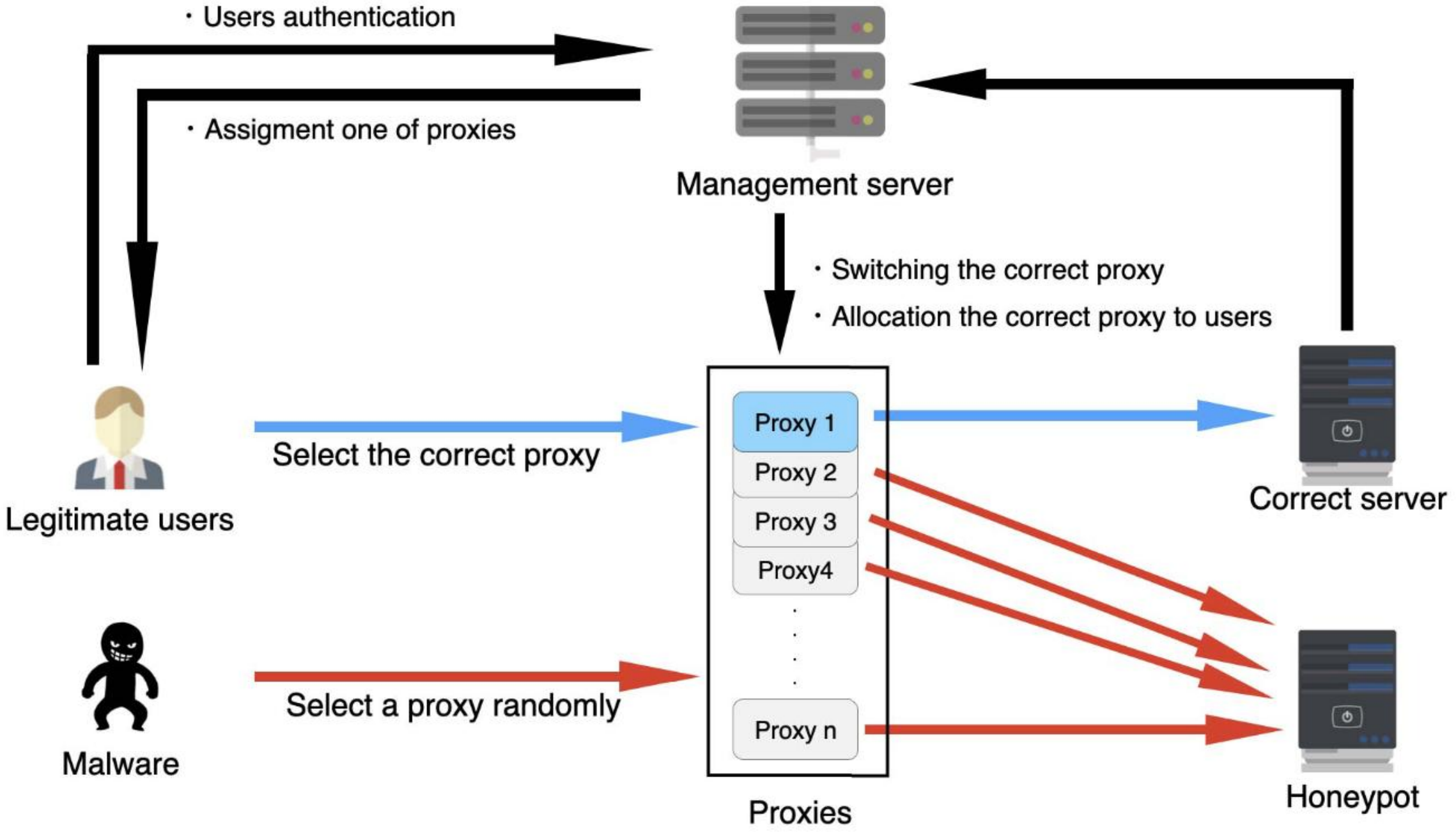
So if malware can be detected & removed from the networks during lurking period,the system can be protected without causing serious damage.



Advanced Persistent Threat (APT) attack lifecycle

Malware has infiltrated a company network and is hiding in order to further expand its infiltration




• Users authentication
• Assigment one of proxies
Management server
• Switching the correct proxy
• Allocation the correct proxy to users
Legitimate users
Select the correct proxy
Proxy 1
Proxy 2
Proxy 3
Proxy4
Proxy n
Correct server
Malware
Select a proxy randomly
Honeypot
Proxies

- The legitimate users complete the authentication and are assigned to correct proxy by the authentication server.They can access the correct server through the proxy while the malware does not know it and chooses a proxy randomly.
- The probability that he malware can access the correct server is expected to be inversely proportional to the number of proxies running.

Malware Detection

Experiment Setup:

- Malware randomly selects a proxy from available options.
- Experiment conducted number of times with varying proxy counts: 2, 4, 8, 16, 32, 64.
- Goal: Measure how often malware selects an incorrect proxy (redirected to honeypot).

Key Findings:

- Detection Probability $P = 1 - 1/N$ (where N is the number of proxies).
- Detection probability increases as the number of proxies increases.

Experimental vs. Theoretical Results:

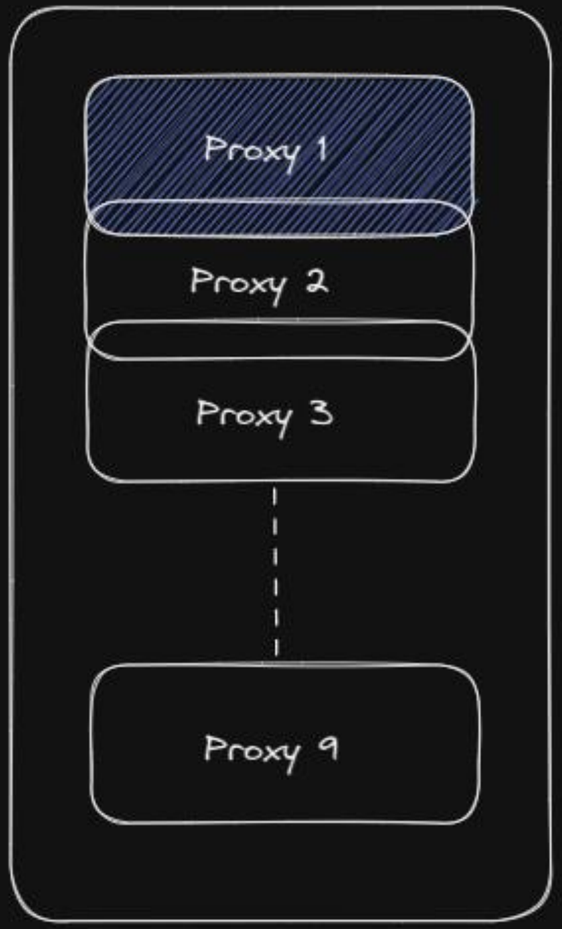
TOTAL PROXIES	THEORETICAL PROBABILITY	EXPERIMENTAL DETECTION PROBABILITY
2	0.5	0.4963
4	0.75	0.7558
8	0.875	0.8738
16	0.9375	0.9325
32	0.96875	0.9657
64	0.984375	0.9854

Conclusion:

- Higher proxy count leads to higher detection probability.
- Experimental results align with theoretical predictions.

EFFECTIVE ARRANGEMENT OF PROXIES

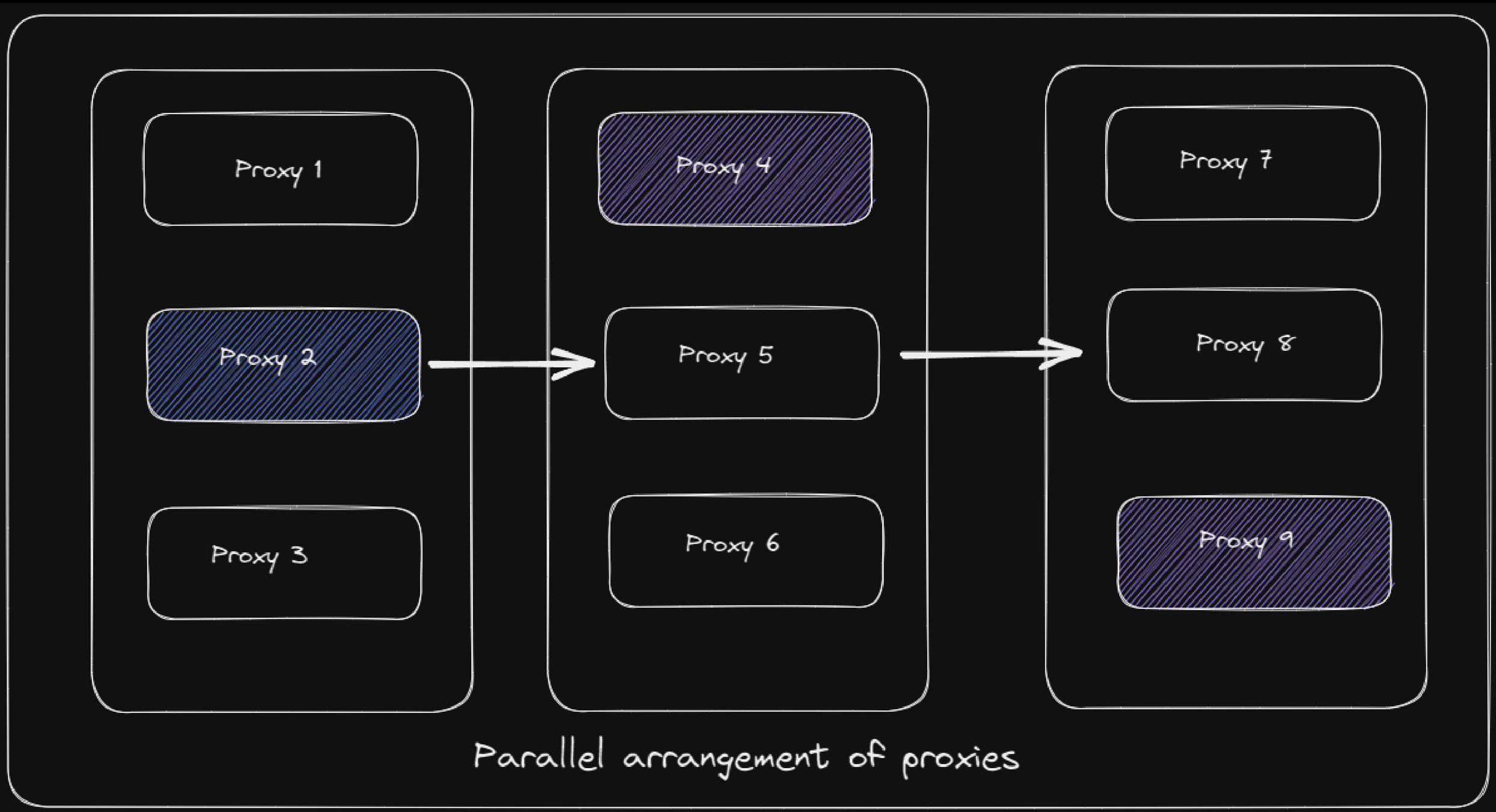
TO IMPROVE THE MALWARE DETECTION RATE WITHOUT INCREASING THE NUMBER OF PROXIES.



Serial arrangement of proxies

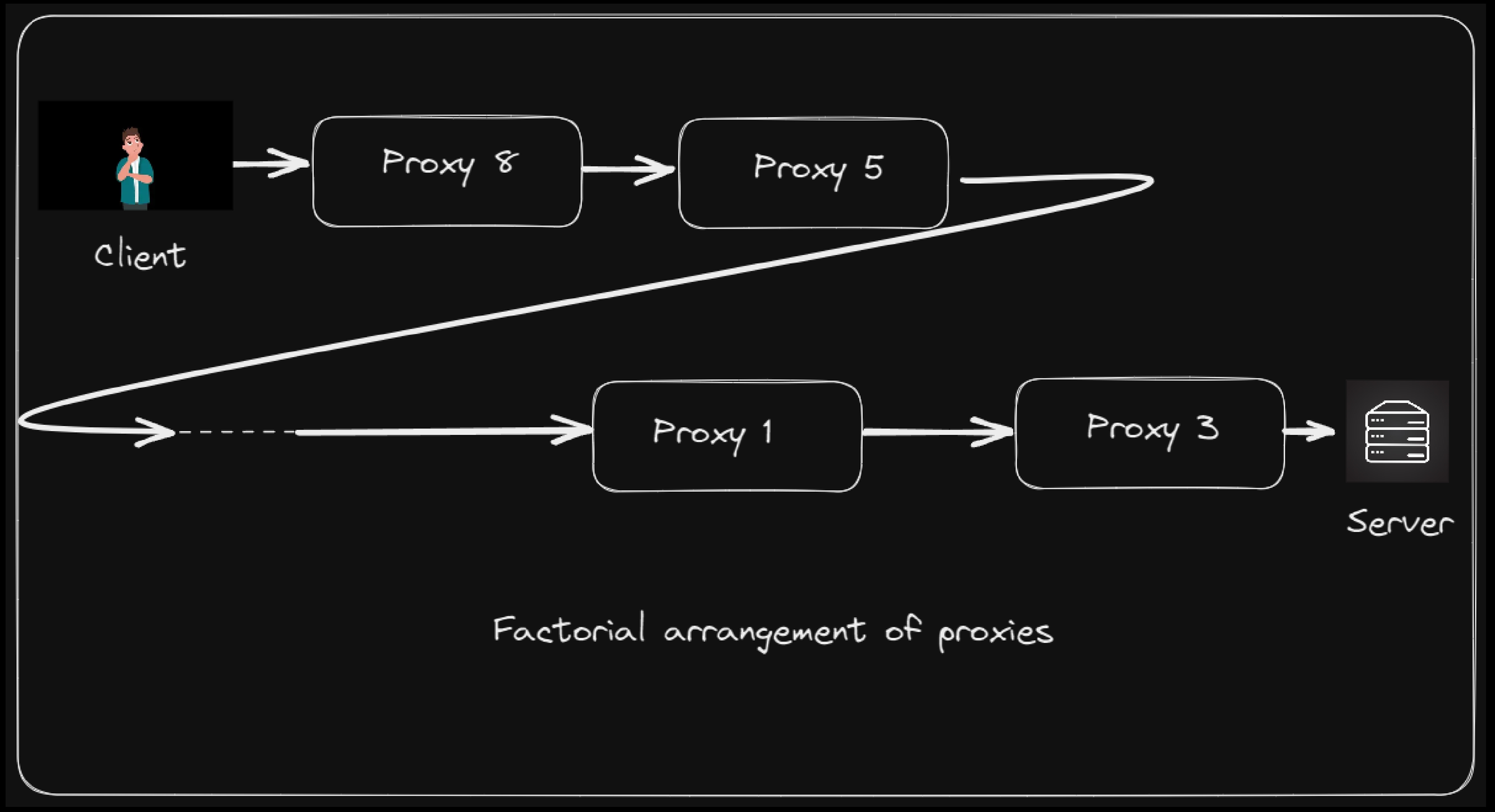
Total number of proxies: 9

The malware detection (P) = 8/9


Proxy 1
Proxy 2
Proxy 3
Proxy 4
Proxy 5
Proxy 6
Proxy 7
Proxy 8
Proxy 9
Parallel arrangement of proxies

Probability of selecting proxies in the incorrect order:

$$P = 1 - (1/3 \times 1/3 \times 1/3) = 26/27$$


Client
Proxy 8
Proxy 5
Proxy 1
Proxy 3
Server
Factorial arrangement of proxies

Proxy selection method is: 9!

$$P = 362879/362880.$$

MTD to counter to Ransomware.

Common characteristics of Ransomware:

- Encryption of Files
- Ransom Demand: Attackers demand payment (usually in cryptocurrency) for decryption keys.
- File Renaming: It often changes file extensions to signal encryption (e.g., `.locked`, `.crypt`).
- Ransom Note: Displays a message or pop-up with payment instructions.
- Data Exfiltration: Some ransomware also steals sensitive data before encrypting it.
- Disabling Security: It often disables antivirus, backup, or other security measures.

Let’s see how Ransomware looks like

Windows (Snapshot 1) [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Recycle Bin

Khufiyawor...

lolbhootja...

passwords...

Ransomwar...

Ransomware.
wannacry.exe

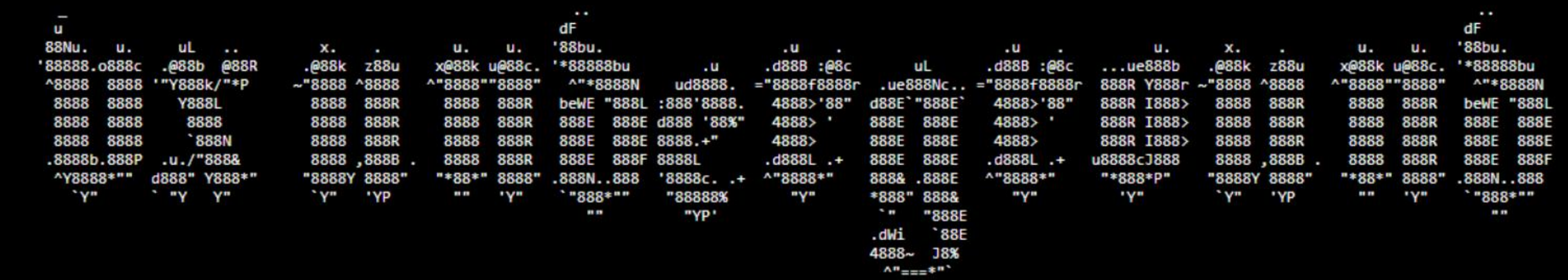
Windows 10 Enterprise Evaluation
Windows License valid for 76 days
Build 19041.vb_release.191206-1406

Type here to search

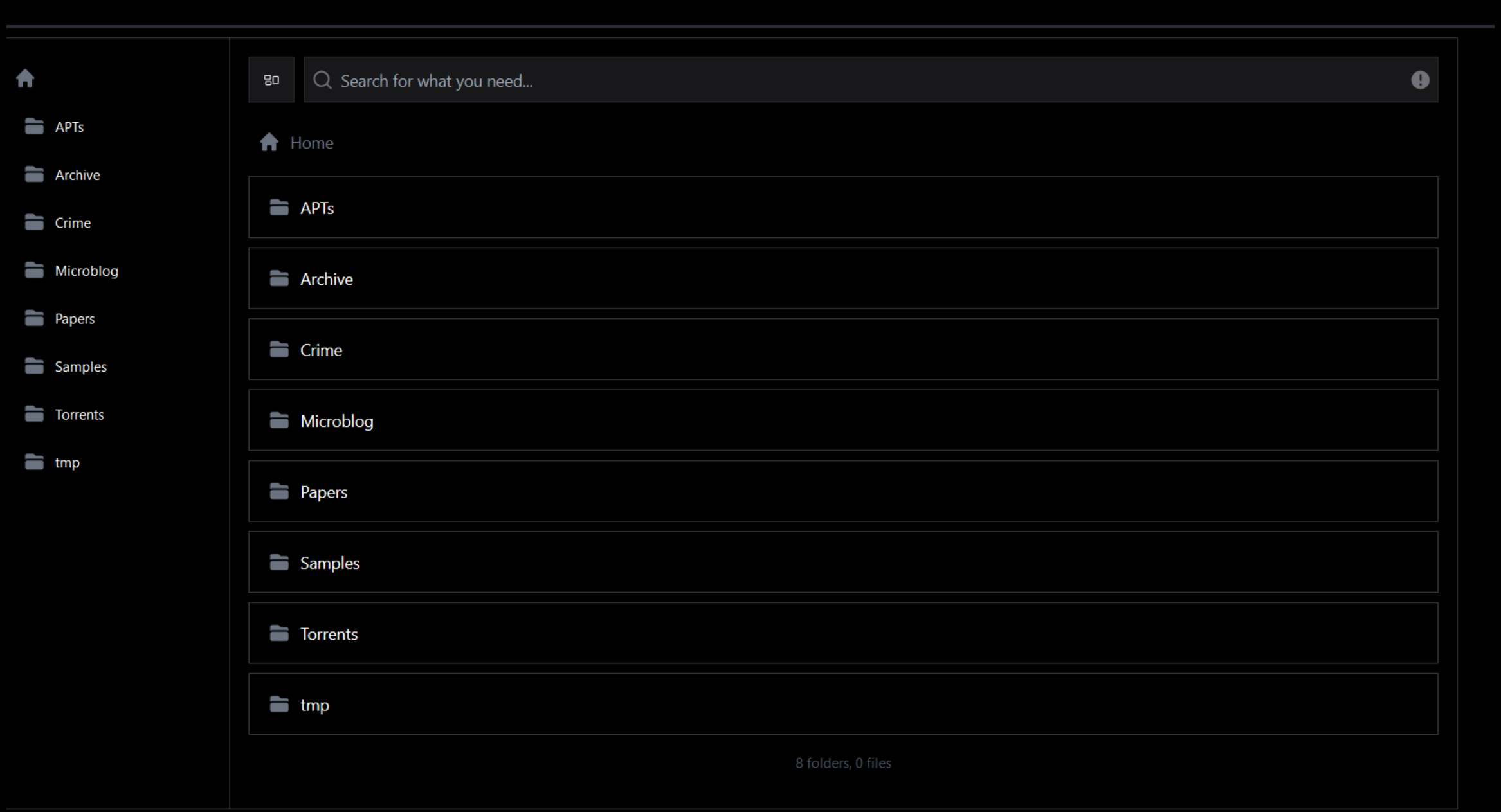
25°C Clear

9:28 AM
10/16/2024

Right Ctrl



Provided FREE to you thanks to our wonderful sponsors

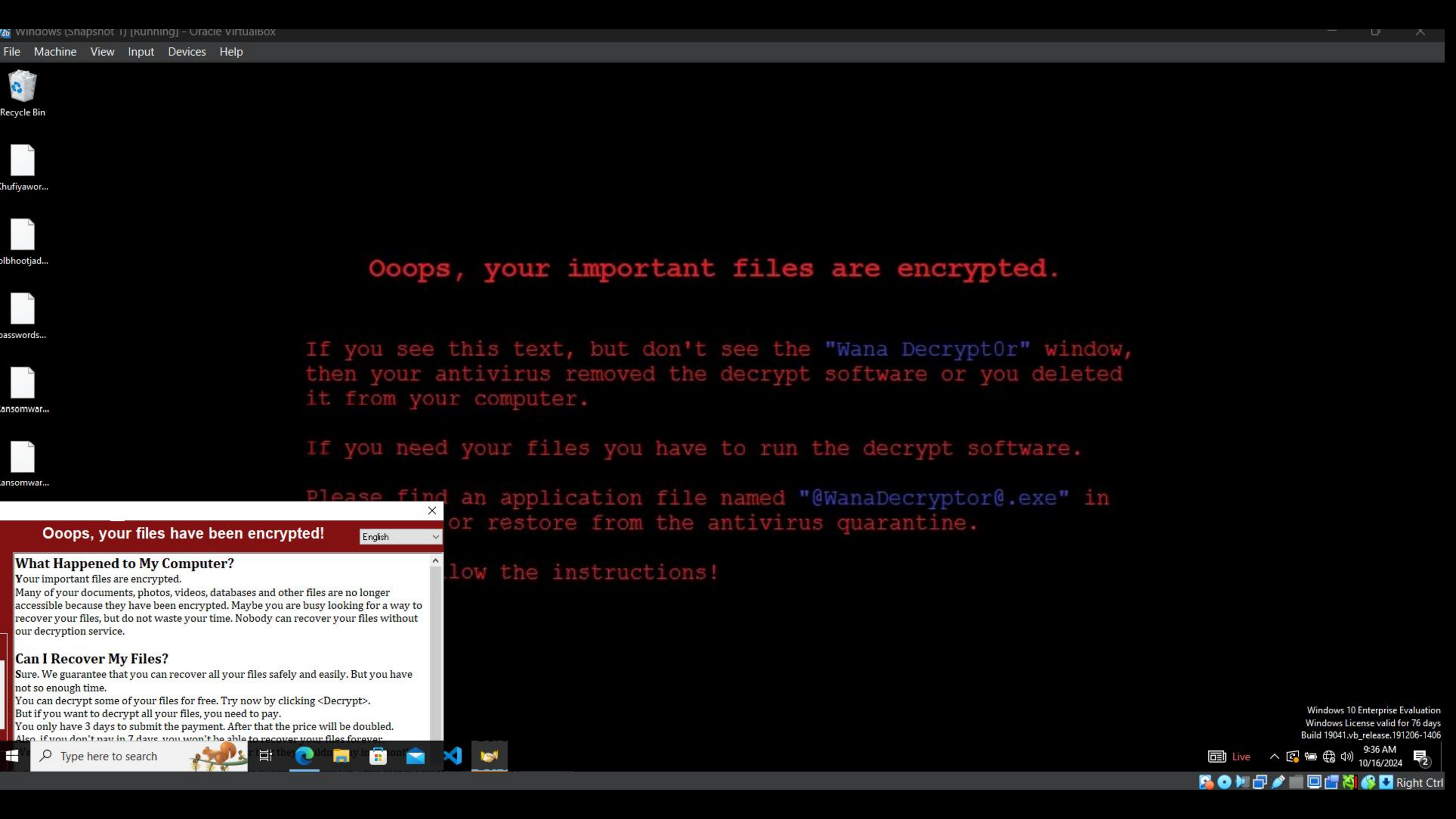

Search for what you need...
Home
APTs
Archive
Crime
Microblog
Papers
Samples
Torrents
tmp
8 folders, 0 files

slido

Please download and install the Slido app on all computers you use

Are you interested in attending a workshop to learn how to set up your own malware lab?

ⓘ Start presenting to display the poll results on this slide.


Windows (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
Khufiyawor...
olbhootjad...
passwords...
ansomwar...
ansomwar...
Ooops, your important files are encrypted.
If you see this text, but don't see the "Wana DecryptOr" window,
then your antivirus removed the decrypt software or you deleted
it from your computer.
If you need your files you have to run the decrypt software.
Please find an application file named "@WanaDecryptor@.exe" in
or restore from the antivirus quarantine.
low the instructions!
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
Type here to search
Windows 10 Enterprise Evaluation
Windows License valid for 76 days
Build 19041.vb_release.191206-1406
Live
9:36 AM
10/16/2024
Right Ctrl


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

Windows (Snapshot 1) [Running] - Oracle VirtualBox

File Machine View Input Devices Help

Recycle Bin

Khufiyawor...

lolbhootja...

passwords...

Ransomwar...

Ransomware.
wannacry.exe

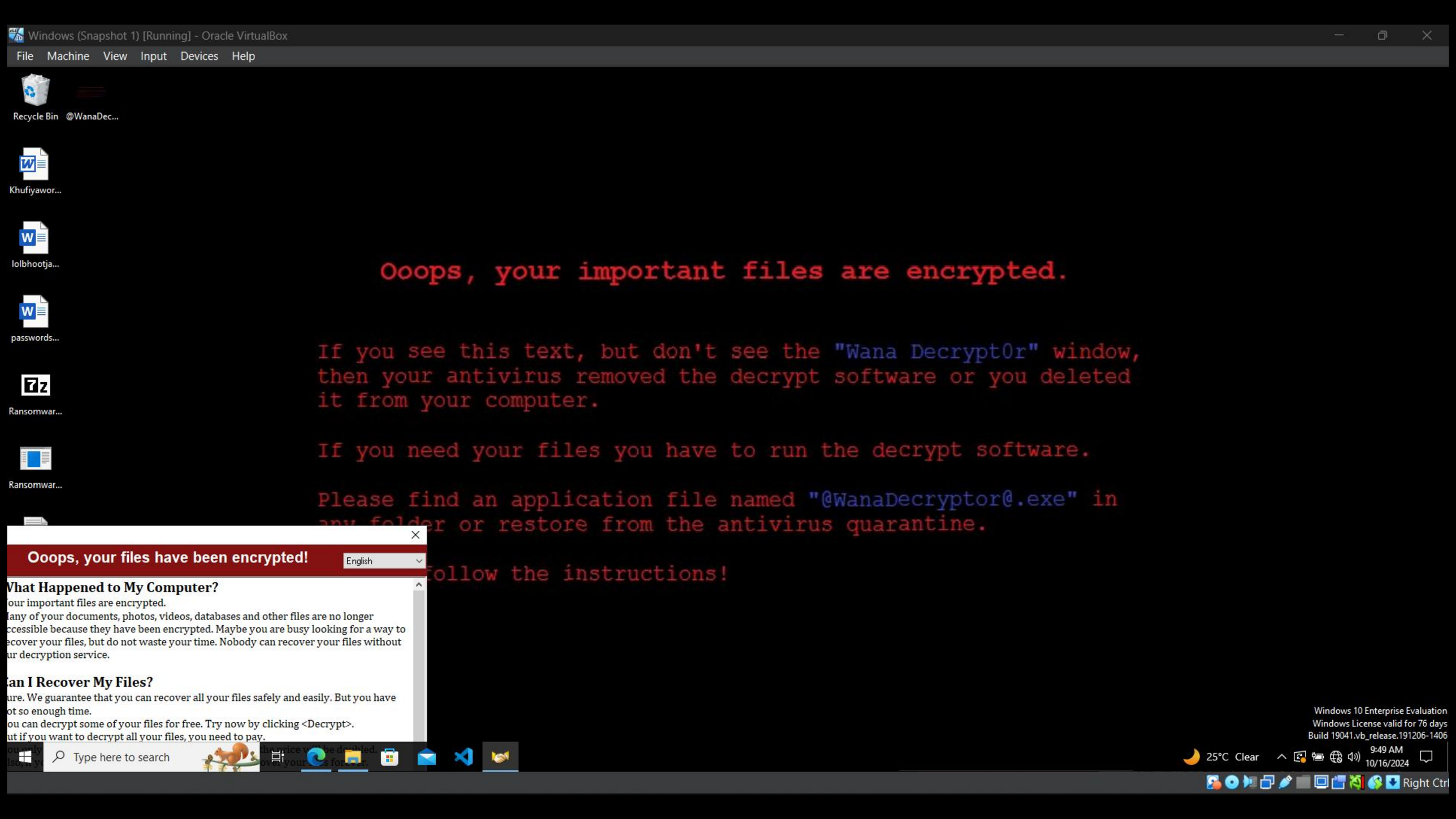
Windows 10 Enterprise Evaluation
Windows License valid for 76 days
Build 19041.vb_release.191206-1406

Type here to search

25°C Clear

9:27 AM
10/16/2024

Right Ctrl


Windows (Snapshot 1) [Running] - Oracle VirtualBox
File Machine View Input Devices Help
Recycle Bin
@WanaDec...
Khufiyawor...
lolbhootja...
passwords...
Ransomwar...
Ransomwar...
Ooops, your important files are encrypted.
If you see this text, but don't see the "Wana DecryptOr" window,
then your antivirus removed the decrypt software or you deleted
it from your computer.
If you need your files you have to run the decrypt software.
Please find an application file named "@WanaDecryptor@.exe" in
any folder or restore from the antivirus quarantine.
follow the instructions!
Ooops, your files have been encrypted!
English
What Happened to My Computer?
our important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer
ccessible because they have been encrypted. Maybe you are busy looking for a way to
ecover your files, but do not waste your time. Nobody can recover your files without
ur decryption service.
an I Recover My Files?
ure. We guarantee that you can recover all your files safely and easily. But you have
ot so enough time.
ou can decrypt some of your files for free. Try now by clicking <Decrypt>.
ut if you want to decrypt all your files, you need to pay.
Type here to search
25°C Clear
9:49 AM
10/16/2024
Windows 10 Enterprise Evaluation
Windows License valid for 76 days
Build 19041.vb_release.191206-1406
Right Ctrl

बैकग्राउंड में क्या हुआ?

- The tool changes file extensions to random ones.
- New extensions are registered in the system.
- Example: ".pdf" files may be renamed to "defcon" but still work like ".pdf".
- Original ".pdf" files remain unaffected.
- This confuses ransomware that looks for specific file extensions.

MTD to counter advanced in-memory malware.

Why it’s important talking about In-memory malware attacks ??

Why it’s important talking about In-memory malware??

- Over 40% of attacks are in memory

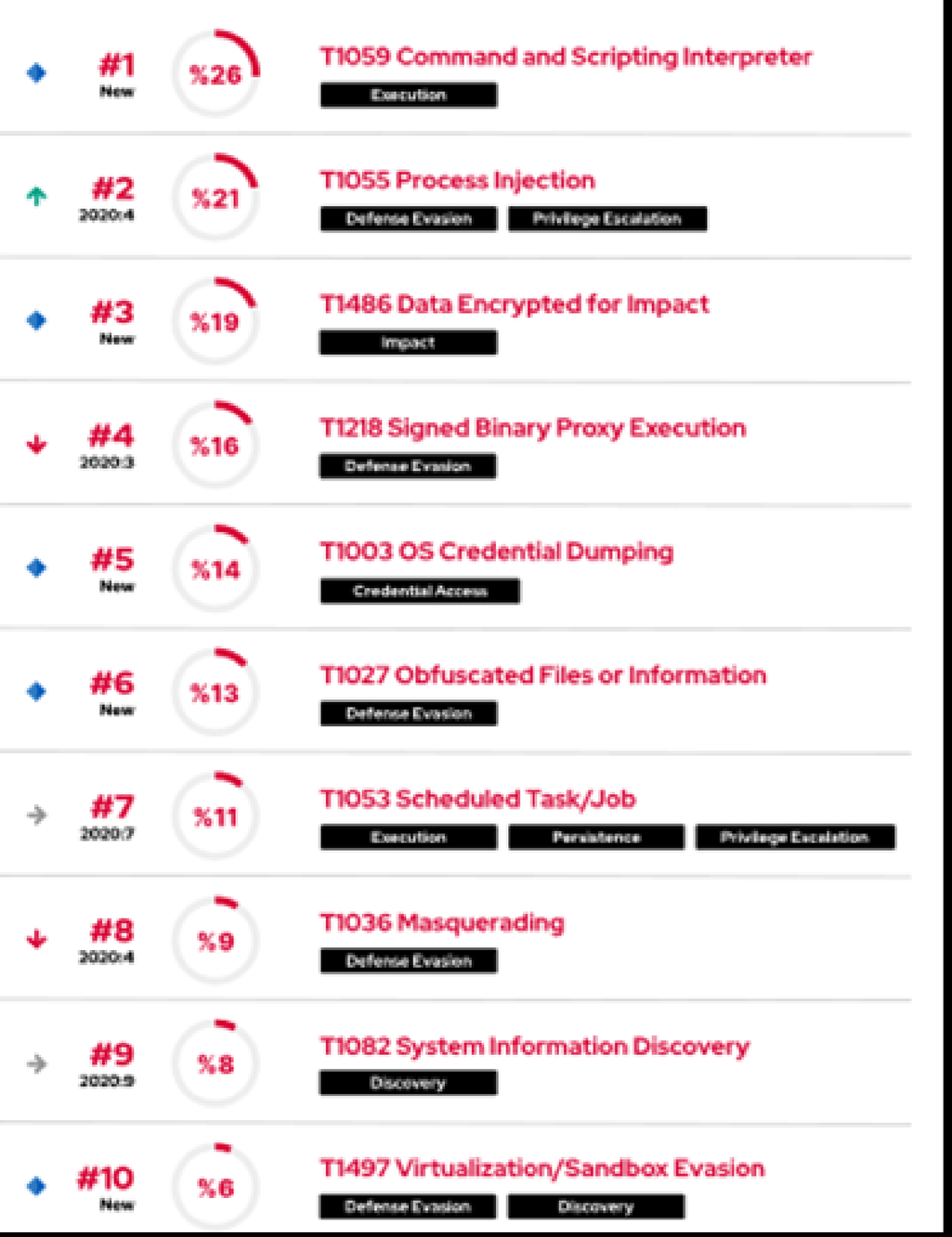
Why it’s important talking about In-memory malware??

- Over 40% of attacks are in memory
- 75% of breach are caused by file-less, in-memory attacks

Why it’s important talking about In-memory malware??

- Over 40% of attacks are in memory
- 75% of breach are caused by file-less, in-memory attacks
- Upto 80% of attacks happens on Endpoints

* The 2017 State of Endpoint Security, Risk Institute, November 2017



POINTER TO PONDER

- Defense Evasion is the Most Common ATT&CK Tactic
- Inherit NGAV, EDR, EPP, XDR challenges
- IN-MEMORY IS NOW WHERE ATTACKERS PREFER TO TARGET
- Four of the top six ATT&CK techniques observed are in-memory

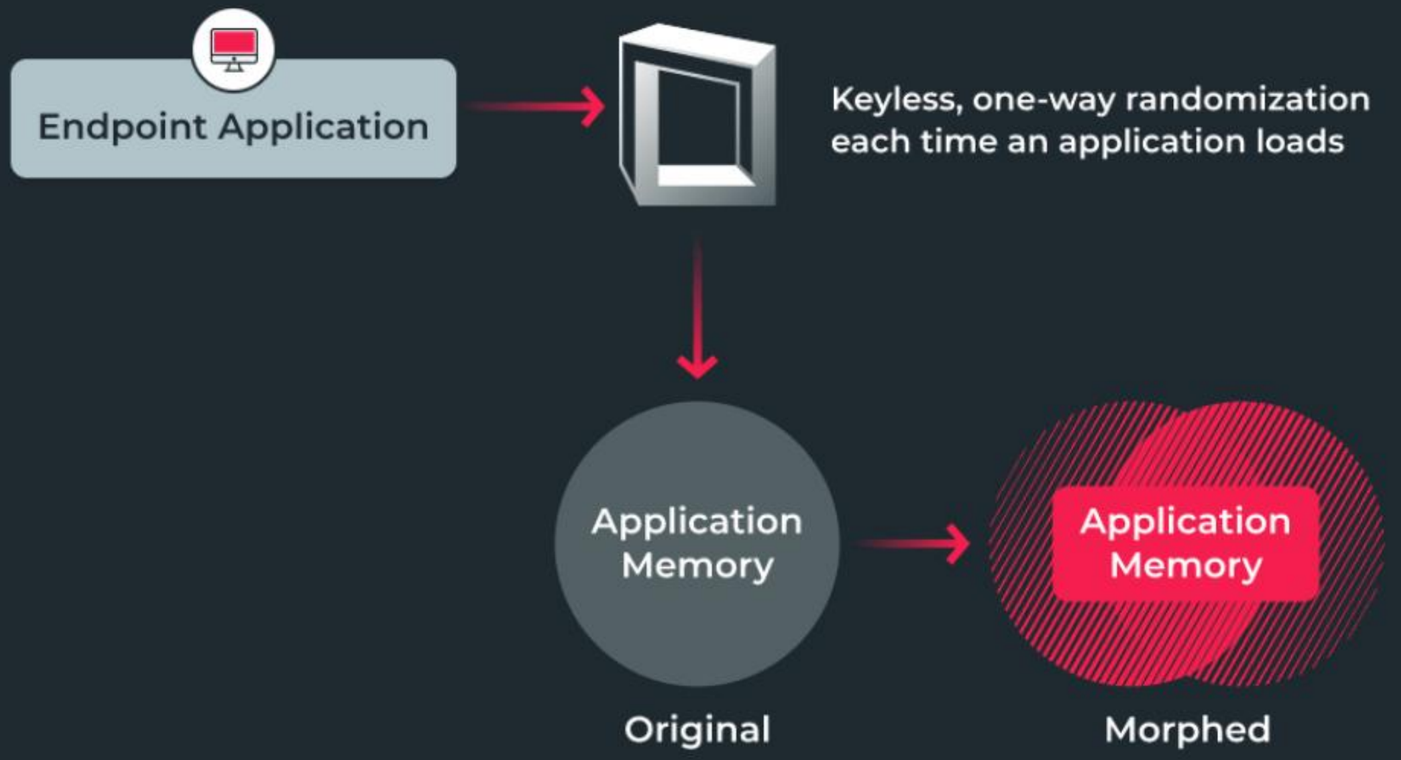
Traditional Malware Detection and Its Limitations

- Reliance on Signatures and Patterns: Traditional tools (AV, NGAV, EPP, EDR, XDR) depend on detecting known malware signatures and attack patterns.
- Focus on Disk-Based Artifacts: These tools are effective against malware that leaves traces on disk or affects the OS.
- Attackers increasingly use methods that avoid the disk and OS, instead hijacking legitimate processes and executing payloads directly in memory

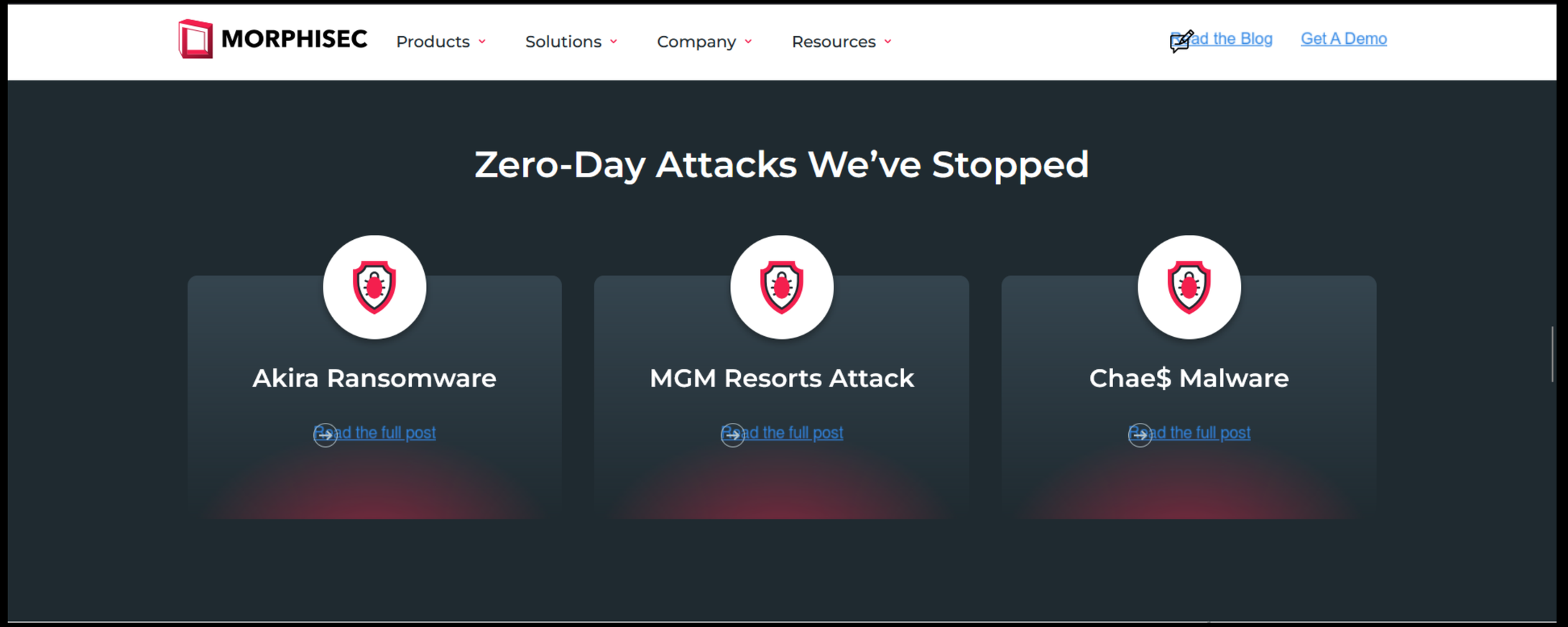
It will be proactive, prevention-first approach.!

MORPHISEC Products Solutions Company Resources Read the Blog Get A Demo

Morph & Conceal | Protect & Deceive | Prevent & Expose Attacks



As an application loads to the memory space, Morphisec morphs the process structures, making the memory constantly unpredictable to attackers.


MORPHISEC
Products
Solutions
Company
Resources
Read the Blog
Get A Demo
Zero-Day Attacks We've Stopped
Akira Ransomware
Read the full post
MGM Resorts Attack
Read the full post
Chae$ Malware
Read the full post

THANK YOU

References

1. https://www.dhs.gov/archive/science-and-technology/csd-mtd
2. Navas, Renzo E., et al., "MTD, where art thou? a systematic review of moving target defense techniques for IoT.", IEEE internet of thingsjournal 8.10, 2020, 7818-7832
3. Higgins, Martin, Fei Teng, and Thomas Parisini, "Stealthy MTD againstunsupervised learning-based blind FDI attacks in power systems.", IEEE Transactions on Information Forensics and Security 16, 2020, 1275-1287
4. https://american-cse.org/csci2022-ieee/pdfs/CSCI2022-2lPzsUSRQukMlxf8K2x89I/202800b072/202800b072.pdf