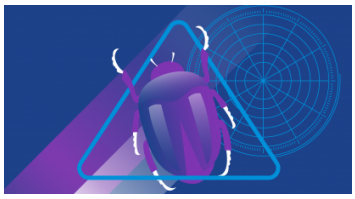


Threat Analysis Unit | Threat Intelligence

Jupyter Rising: An Update on Jupyter Infostealer

Swee Lai Lee, Bria Beathley, Abe Schneider, Alan N... /
November 6, 2023 / 18 min read

Contributor: Nikki Benoit

Executive Summary

New Jupyter Infostealer variants continue to evolve with simple yet impactful changes to the techniques used by the malware author. This improvement aims to avoid detection and establishes persistence, enabling the attacker to stealthily compromise victims. The Carbon Black MDR Team has contained countless Jupyter Infostealer infections over the years. This malware continues to be one of the top ten infections we've detected in our clients' network primarily targeting the Education and Health sectors.

The team has discovered new waves of Jupyter Infostealer attacks which leverage PowerShell command modifications and signatures of private keys in attempts to pass off the malware as a legitimately signed file. Over the last two weeks, the number of Jupyter Infostealer infections that we have observed has steadily risen, now totaling 26 infections. Malware researchers such as SquiblydooBlog have also noted the recent changes.

History

Jupyter Infostealer (aka Yellow Cockatoo, Solarmarker, Polazert) is a malware variant that was first detected in late 2020. It has continued to evolve, changing its delivery method to evade detection. Targeting Chrome, Edge, and Firefox browsers, Jupyter infections use SEO poisoning and search engine redirects to encourage malicious file downloads that are the initial attack vector in the attack chain. The malware has demonstrated credential harvesting and encrypted command-and-control (C2) communication capabilities used to exfiltrate sensitive data.

Certificate Manipulation

These files are signed with a valid certificate to further evade detection. The recent Jupyter infections utilize multiple certificates to sign their malware which, in turn, can

allow trust to be granted to the malicious file, providing initial access to the victim's machine.
Recent Signers:

- ТОВ "Чеб"
- ТОВ "Софт Енжін юа"
- ТОВ "Трафік Девелоп ЮА"

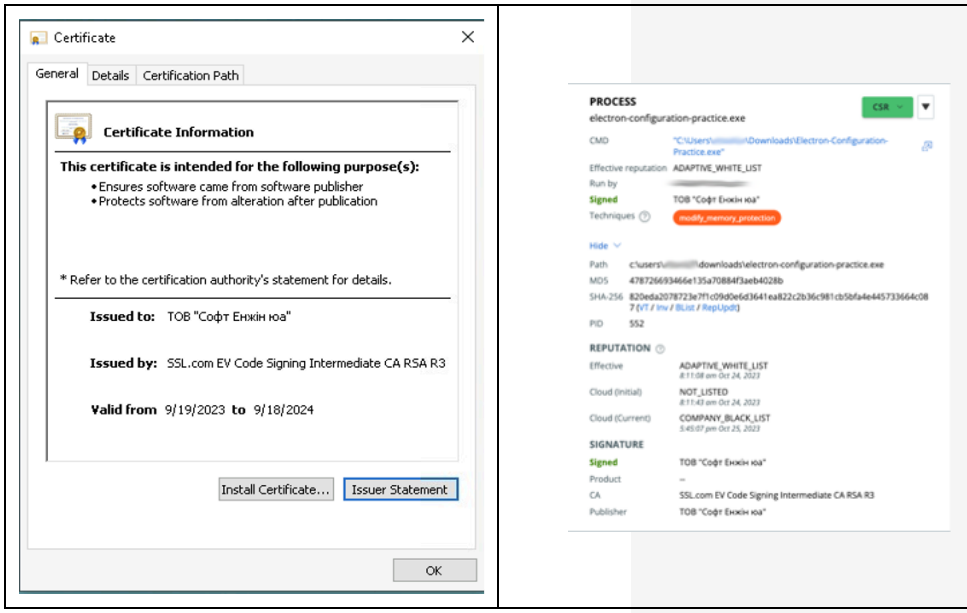


Figure 1: Certificate Information

Crafty threat actors are particularly interested in obtaining such certificates; even security analysts may inadvertently place trust in such software due to the semblance of authenticity provided by these certificates.

Common Delivery Methods

Jupyter Infostealer, like many other malware, can be delivered through various methods. Common delivery methods include: malicious websites, drive-by downloads, and phishing emails. Users may unknowingly download Jupyter Infostealer when visiting compromised websites or by clicking on malicious ads. The most common applications we see used to download this malware are: Firefox, Chrome, and Edge web browsers.

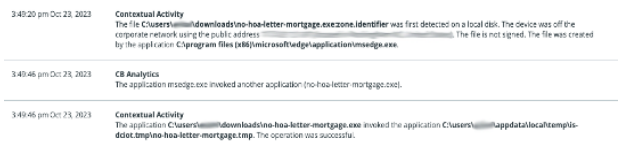


Figure 2: No-Hoa-Letter-Mortgage.exe invokes No-Hoa-Letter-Mortgage.tmp file

When a user gets tricked into downloading this Infostealer, the executable can then get invoked by their browser.

We also observed the initial files with different naming conventions:

- *An-employers-guide-to-group-health-continuation.exe*
- *How-To-Make-Edits-On-A-Word-Document-Permanent.exe*
- *052214-WeatherPro-Power-Patio-Sport-Replacement-Fabric.exe*
- *Iv-Calculations-Practice-Questions-Pdf.exe*
- *Sister-Act-Libretto-Pdf.exe*
- *Coaches-Gift-Donations.exe*
- *Electron-Configuration-Practice.exe*
- *Environmental-Accounting-Education-Requirements.exe*
- *American-Born-Chinese.exe*

Fake Installer

The above executables are examples of installation files created by InnoSetup – an open source compiler used to create installation packages in Windows OS. These new infections typically include this installer-bundle.exe file which retains the same hash although their file names may vary.

Autodesk

During our recent investigation, we identified an incident where a signed Autodesk Create Installer was deployed by the installer-bundle.exe. Autodesk, a software frequently exploited in past cyber attacks, was utilized as a Remote Desktop application on the victims' devices.

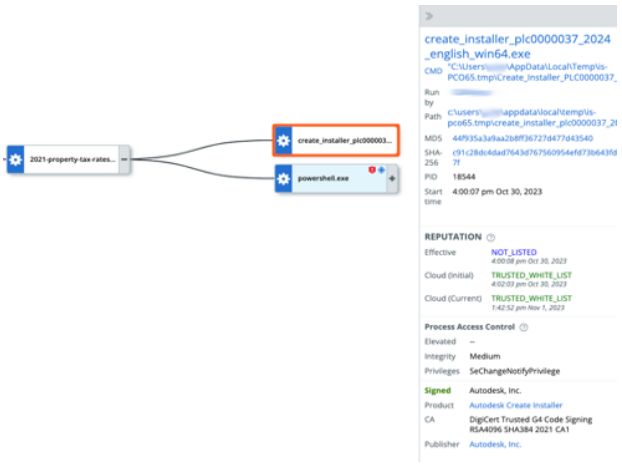


Figure 3: Installer-bundle.exe dropping AutoDeck Create Installer

Moments after, **No-Hoa-Letter-Mortgage.tmp** executes **powershell.exe** which then makes a connection to 185[.]243.112.60, a C2 server located in the Netherlands.

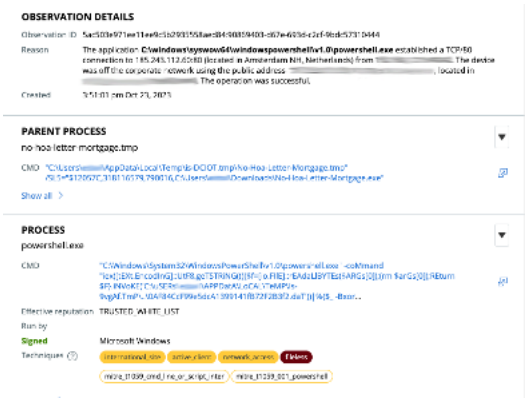


Figure 4: Encoded Powershell command

Multiple files are then created and opened with write privileges, including the **.dat** file shown in the PowerShell command above. These files are typically stored in the %Temp% directory.

Figure 5: Events seen in Process Analysis page in Enterprise Endpoint Detection and Response

The PDF file that the malware drops into the %Temp% folder, as seen in the image above, is used as a decoy for the victim.

Figure 6: A screenshot of budget_fy2024.pdf seen by the victim

These same files then get deleted a few minutes after initial infection.

Figure 7: Files seen being deleted

After a foothold is established on the user's device, PowerShell is used to immediately establish multiple network connections to their C2 server after executing the following command:

Figure 8: PowerShell commands seen attempting to reach out to C2 server

The above PowerShell command was executed to decrypt the **.DAT** file (0AF84CcF99e5dcA1399141fB72F2B3f2.daT) with a custom XOR key. The below image shows the snippet of the decoded PowerShell script:

Figure 9: Decoded PowerShell script

The above PowerShell script was used to decode the Infostealer payload and load the DLL payload in-memory using the Reflection.Assembly::load method.

Figure 10: Jupyter Infostealer process chart

Carbon Black Detection and Prevention

The Carbon Black MDR Team routinely scans for new adversary techniques used to bypass detection. Once a threat is identified, our team acts quickly to contain the attack and prevent exfiltration of valuable data.

Figure 11: Analysts implement a blocking policy to prevent Jupyter from executing PowerShell, a policy deny action was applied

With MDR analysts watching over our clients 24-hours a day, the team is able to implement prevention rules to identify and contain various versions of Jupyter Infostealer around the clock.

Figure 12: The Events page showing that the Policy Deny action was applied and the operations were blocked by Carbon Black

Summary

Jupyter Infostealer exhibits a remarkable ability to evolve and adapt. These modifications seem to enhance its evasion capabilities, allowing it to remain inconspicuous. As cyber defenses strengthen, malicious software finds new avenues to breach and infect systems leaving us vulnerable to newer renditions of commonly seen older attacks.

Managed Threat Hunting

As we continue to see malware evolve, some get phased out and others adapt. This blog post is meant to observe and document the behavioral patterns and changes of Jupyter Infostealer. With this we have seen the improvements of the evasive abilities Jupyter uses in attempts to stay under the radar and continue to silently infect victims.

Carbon Black adopts a different approach, focusing on both pre and post-exploit defense. This strategy proves more effective against Jupyter Infostealer, ensuring detection, prevention, and containment.

Carbon Black is particularly effective against Jupyter Infostealer due to its innovative approach to endpoint security. Unlike traditional antivirus (AV) solutions that rely solely on static signatures or hashes to detect malware, Carbon Black utilizes advanced techniques and behavioral analysis for threat detection. Here's why Carbon Black is a superior endpoint protection to use against Jupyter Infostealer:

- **Dynamic Detection Methods:** Carbon Black employs dynamic detection methods, such as behavioral analysis and machine learning algorithms, to identify malicious behavior patterns. This proactive approach allows it to detect new and evolving threats such as Jupyter

Infostealer even when their specific signatures or hashes are unknown.

- **Focus on Pre and Post-Exploit Defense:** Carbon Black focuses on both pre-exploit and post-exploit defense. While traditional AVs primarily concentrate on pre-exploit measures, Carbon Black also monitors activities after a potential breach. This comprehensive approach enables it to identify and mitigate Jupyter Infostealer malicious activities throughout the attack lifecycle.
- **Adaptability to Unique Attacks:** Jupyter Infostealer, being a malware-as-a-service, allows attackers to customize their attacks resulting in unique configurations for each instance. Carbon Black's adaptive and behavioral analysis can recognize these custom configurations and detect Jupyter Infostealer variants regardless of the specific parameters set by the attacker.
- **Containment Capabilities:** Carbon Black not only detects malware but also offers effective containment measures. When Jupyter Infostealer is detected, Carbon Black can isolate the infected system, preventing the malware from spreading further within the network. This containment feature helps prevent widespread damage and data breaches.
- **Continuous Updates and Threat Intelligence:** Carbon Black continuously updates its threat intelligence database, incorporating information about emerging threats and attack techniques including those used by Jupyter Infostealer. This up-to-date knowledge enhances its ability to recognize and thwart the latest variants of the malware.
- **Adaptive Response:** Carbon Black's Managed Detection and Response products provide an adaptive response mechanism. In the event of a Jupyter Infostealer attack, it can respond dynamically, adapting its defense strategies based on the evolving threat landscape. This adaptability is crucial in dealing with constantly changing malware tactics.
- **Managed Threat Hunting:** Carbon Black's newly released Managed Threat Hunting product provides proactive threat hunting on emerging threats. The Managed Threat Hunting product's unique approach to detection and response allows it to quickly detect and respond to threats, including Jupyter Infostealer .

Carbon Black's advanced, dynamic, and comprehensive approach to threat detection and response makes it highly effective against Jupyter Infostealer and other sophisticated malware threats. Carbon Black's ability to adapt, analyze behavior, and contain attacks sets it apart as a robust solution in the fight against evolving cyber threats.

Search Queries

- process_cmdline:*utf8.GeTsTriNG* AND process_cmdline:*ReadAllBytes*
- process_name:powershell.exe AND process_cmdline:\-bxor AND process_cmdline:utf8.getstring AND process_cmdline:readallbytes
- hash:820eda2078723e7f1c09d0e6d3641ea822c2b36c981cb5bfa4e445733664c087 OR 95a96d21f89b5e73ad41c5af5381f54a2697abd0c8490b4fd180ad88e9677452 OR 32e0c3db78cdeaa026b8b9ed9c3e4f599eb5d9cb4184aaacae8ec94a0c1be438 OR ad7098b4882cdd187a2c2bdf87f6e4cb6c76017975a135cf9c9dcd49ce1f30d7 OR c083bf80cfc91f4e3c696bab27760163b9b7621ff4e1230b8129d44b52ccf79a OR 39102fb7bb6a74a9c8cb6d46419f9015b381199ea8524c1376672b30fffd69d2 OR fee1e684cc9588c9aea22c48e9745d0f3150479b2c094c0de598247487fc3f89 OR 7d57b32e3753a28d2e106392fef0c02ec549062f607563732a64abb4ad949fde
- netconn_ipv4:146.70.101.83 OR 239.255.255.250 OR 224.0.0.251 OR 91.206.178.10 OR 78.135.73.176 OR 185.243.112.60 OR 146.70.71.13 OR 146.70.121.88

Indicators of Compromise (IOC)

Name	SHA256 Hash
no-hoa-letter-mortgage.exe	820eda2078723e7f1c09d0e6d3641ea822c2b36
no-hoa-letter-mortgage.tmp	95a96d21f89b5e73ad41c5af5381f54a2697abd0c
an-employers-guide-to-group-health-continuation.exe	32e0c3db78cdeaa026b8b9ed9c3e4f599eb5d9c
an-employers-guide-to-group-health-continuation.tmp	ad7098b4882cdd187a2c2bdf87f6e4cb6c760179
316798e6deddba410e710d355c6f6f2a.pdf	c083bf80cfc91f4e3c696bab27760163b9b7621ff
Scum-and-villainy-rpg-pdf.exe	39102fb7bb6a74a9c8cb6d46419f9015b381199ea
Job-satisfaction-in-relation-to-communication-in-health-care.tmp	fee1e684cc9588c9aea22c48e9745d0f3150479b
job-satisfaction-in-relation-to-communication-in-health-care.exe	7d57b32e3753a28d2e106392fef0c02ec549062f

IPs/Domains	
146[.]70.101.83	239[.]255.255.250

224[.]0.0.251	91[.]206.178.10
78[.]135.73.176	185[.]243.112.60
146[.]70.71.13	146[.]70.121.88

MITRE ATT&CK TIDs

TID	Tactics	Technique
T1204.002	Execution	User Execution: Malicious File
T1059.001	Execution	Command and Scripting Interpreter: PowerShell
T1055	Privilege Escalation	Process Injection
T1547.001	Persistence,Privilege Escalation	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder
T1564.003	Defense Evasion	Hide Artifacts: Hidden Window
T1620	Defense Evasion	Reflective Code Loading
T1027.011	Defense Evasion	Obfuscated Files or Information: Fileless Storage
T1036	Defense Evasion	Masquerading
T1070.004	Defense Evasion	Indicator Removal on Host: File Deletion
T1112	Defense Evasion	Modify Registry
T1082	Discovery	System Information Discovery
T1083	Discovery	File and Directory Discovery
T1552.001	Credential Access	Unsecured Credentials: Credentials In Files
T1005	Collection	Data from Local System
T1105	Command and Control	Ingress Tool Transfer
T1070.001	Command and Control	Application Layer Protocol: Web Protocols
T1041	Exfiltration	Exfiltration Over C2 Channel

Swee Lai Lee
Malware Analyst @ VMware Carbon Black

Bria Beathley

Abe Schneider

Alan Ngo

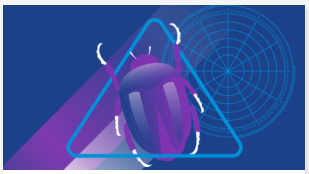
Sean McKnight

Related Articles

Misc

Hunting Vulnerable Kernel Drivers

Takahiro Haruyama / October 31, 2023 / 34 min read



Threat Analysis Unit

An iLUMMAnation on LummaStealer

Fae Carlisle, Bria Beathley, Samantha Saltzman, Ad... / October 18, 2023 / 27 min read

Network Security

VMware vDefend: Latest Enhancements in Advanced Threat Prevention

Prashant Gandhi / October 23, 2024 / 7 min read