Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

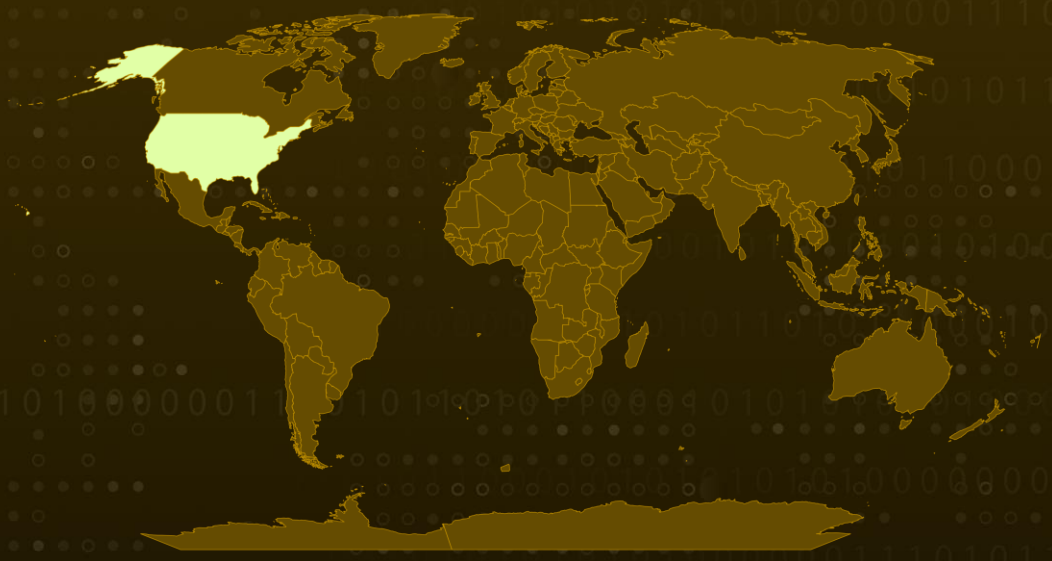
PindOS : a JavaScript dropper unleashing Bumblebee and IcedID malware

Date of Publication	Admiralty Code	TA Number
June 29, 2023	A1	TA2023283

Summary

First appeared: May, 2023
Attack Region: United States
Malware: PindOS, Bumblebee, IcedID
Attack: PindOS, new JavaScript dropper has been spotted in wild. It is specifically engineered to deliver next-stage payloads and is currently deploying infamous malwares like Bumblebee and IcedID.

Attack Regions



Attack Details

#1 PindOS is a sleek JavaScript dropper designed to fetch next-stage payload. It is distributed via social-engineering techniques and once executed, the JavaScript dropper discreetly retrieves and deploys subsequent payloads, such as Bumblebee and IcedID.

#2 PindOS employs a multi-step routine where it generates a User-Agent, calls a URL to fetch its payload, and executes it via the "runll32" command. In case of failure, a secondary URL is invoked, triggering a PowerShell command to run the payload using "rundll32".

#3 Payload is downloaded at “%appdata%/Microsoft/Templates/” as a DAT file with six random numbers as a name. The payloads are generated dynamically leading to new hash each time, this helps in avoiding signature-based detections.

#4 PindOS is found to be deploying Bumblebee and IcedID malware, both are malware loaders and Bumblebee is found to be associated with Conti group. They both are known as primary vectors for other malwares including Ransomware.

#5 Adversaries are employing this multi-stage infection chain to avoid immediate detection and increase the complexity of their malicious activities.

Recommendations

Behavior based Detection: Employ behavior-based security solutions to deal with dynamically generated malware.

Regular Updates: Continuously ensure anti-malware and anti-virus software are loaded with latest detection patterns and have 100% asset coverage.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0005** Defense Evasion	**TA0001** Initial Access	**T1566** Phishing
T1027 Obfuscated Files or Information	**T1059** Command and Scripting Interpreter	**T1218** System Binary Proxy Execution	**T1608** Stage Capabilities
T1204 User Execution	**T1059.007** JavaScript	**T1218.011** Rundll32	**T1608.004** Drive-by Target

Indicators of Compromise (IOCs)

TYPE	VALUE
Sha256	bcd9b7d4ca83e96704e00e378728db06291e8e2b50d68db22efd1f8974d1ca91, 07d2cb0dc0cd353fb210b065733743078e79c4a27c42872cd516a6b1fb1f00d1, 00ec8f3900336c7aeb31fef4d111ee6e33f12ad451bc5119d3e50ad80b2212b0, 15da5b0a65dd8135273124da0c6e52e017e3b54642f87571e82d2314aae97eec, 180a935383b39501c7bdf2745b3a334841f01a7df9d063fecca587b5cc3f5e7a, 24dd5c33b8a5136bdf29d0c07cf56ef0e33a285bb12696a8ff65e4065cb18359, 76c9780256e195901e1c09cb8a37fb5967f9f5b36564e380e7cf2558652f875b, 28c87170f2525fdecc4092fb347acd9b8350ed65e0fd584ce9fc001fd237d523, ac261ac26221505798c65c61a207f3951cc7dce2e1014409d8a765d85bfd91d4, 92506fe773db7472e7782dbb5403548323e65a9eb2e4c15f9ac65ee6c4bd908b, c84c84387f0b9e7bc575a008f36919448b4e6645e1f5d054e20b59be726ee814, ...

TYPE	VALUE
Sha256	7355656f894ae26215f979b953c8fa237dc39af857a6b27754a93adb1823f3b6, 8f40ff286419eb4b0c4d15710dc552afb2c2a227a180f4b4f520d09b05724151, 9101975f7aca998da796fc15a63b36ab8aa0fe0aed0b186aaed06a3383d5f226, 4f0c9c6fc1287ef16f4683db90dd677054a1f834594494d61d765fa3f2e1352c, cb307d7fa6eaac6a975ad64ff966ff6b0b0fdd59109246c2f6f5e8d50a33e93c, 361b0157ef63d362fdd4399288f5f6a0e1536633dfb49c808a3590718c4d8f10, e71c9ac9ddd55b485e636840da150db5cd2791d0681123457bd40623acd8311c, 8ae3be9f09f5fc64ec898a4d6467b2f6e50eaaa26fc460a4f1a9b9566e97a9a7
URL	hxxps://qaswrahc.com/wp-content/out/mn[.]php hxxp://tusaceitesesenciales.com/mn[.]php hxxp://carwashdenham.com/mn[.]php hxxps://intellectproactive.com/dist/out/mn[.]php hxxps://masar-alulaedu.com/wp-content/woocommerce/out/berr[.]php hxxps://egyfruitcorner.com/wp-content/tareq/out/berr[.]php hxxps://tech21africa.com/wp-content/uploads/out/berr[.]php hxxps://www.posao-austrija.at/images/out/lim[.]php hxxps://logisticavirtual.org/wp-content/out/lim[.]php hxxps://adecoco.us/wp-content/out/lim[.]php hxxps://acsdxb.net/wp-content/out/lim[.]php

References

https://www.deepinstinct.com/blog/pindos-new-javascript-dropper-delivering-bumblebee-and-icedid

https://www.hivepro.com/prolific-threat-actor-ta551-using-new-malware-icedid/

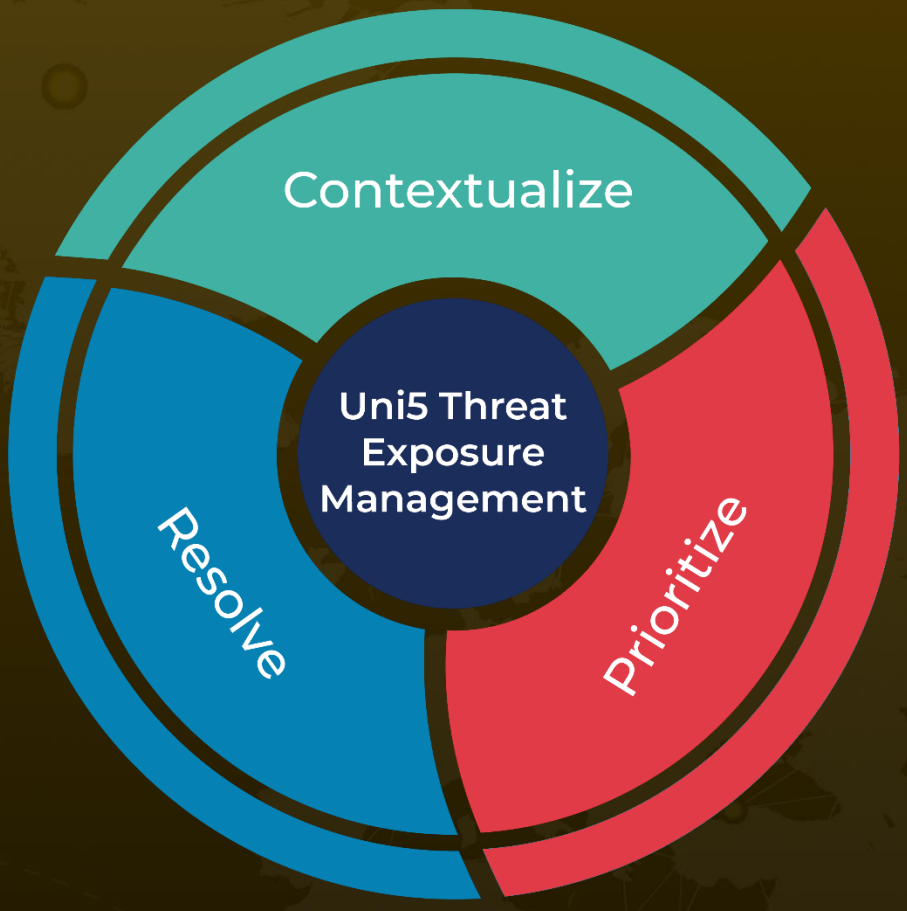
https://www.hivepro.com/malware-distribution-via-google-ppc-by-icedid-botnet-distributors/

https://www.hivepro.com/bumblebee-leverages-zerologon-to-get-domain-controller-access/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

June 29, 2023 • 10:30 PM

More at www.hivepro.com