Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

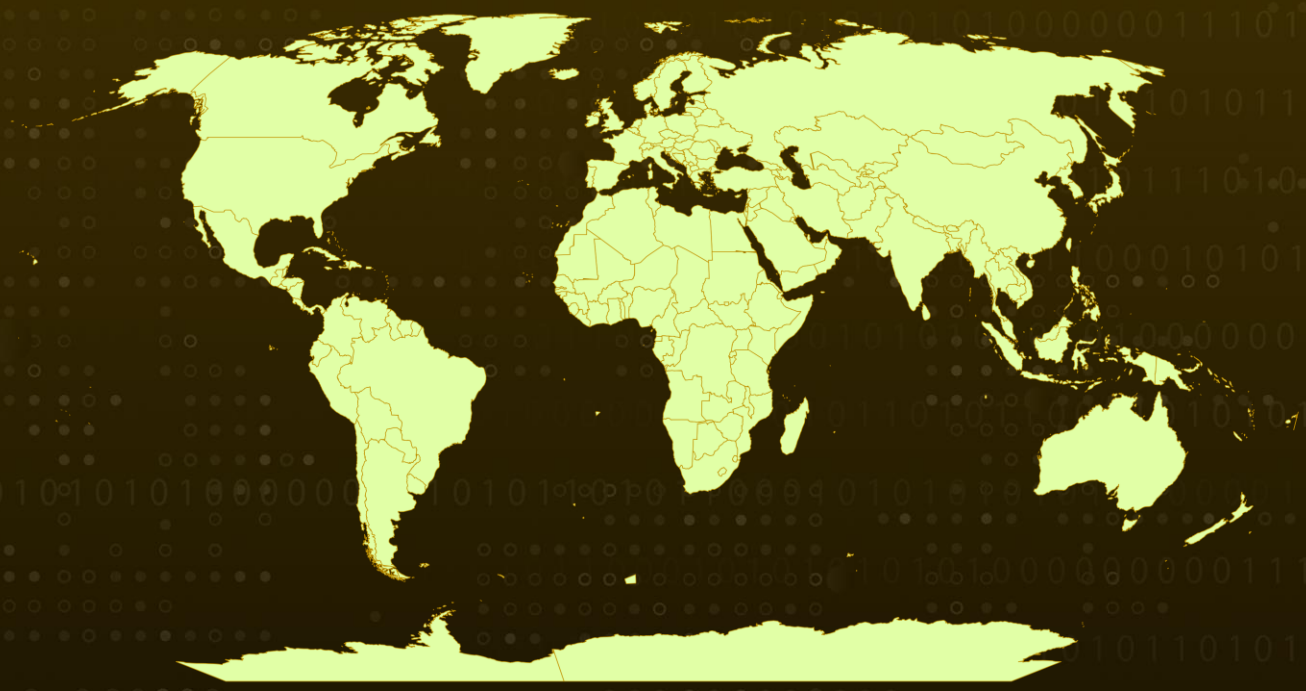
New Ransomware Mimic Emerges in the Wild, Abusing Legitimate Tool for Faster Encryption

Date of Publication	Admiralty Code	TA Number
January 27, 2023	A1	TA2023050

Summary

First appeared: June 2022
Attack Region: Worldwide
Attack: Mimic is a new ransomware that uses the APIs of a legitimate tool called Everything to encrypt target files and has multiple capabilities such as deleting shadow copies, terminating multiple applications and services, and disabling Windows defender.

Attack Regions



Attack Details

#1

Mimic is a new ransomware that was first observed in the wild in June 2022. It targets both Russian and English-speaking users and is equipped with multiple capabilities such as deleting shadow copies, terminating multiple applications and services, and abusing the APIs of a legitimate tool called Everything, a Windows filename search engine developed by Voidtools that offers quick searching and real-time updates for minimal resource usage. This malware is dropped as an executable that drops multiple binaries and a password-protected archive (disguised as Everything64.dll) which when extracted, contains the ransomware payload. It also includes tools that are used for turning off Windows defender and legitimate sdel binaries.

#2

When executed, it will first drop its components to the %Temp%/7zipSfx folder. It will then extract the password protected Everything64.dll to the same directory using the dropped 7za.exe. It will also drop the session key file session.tmp to the same directory, which will be used for continuing the encryption in case the process is interrupted. The ransomware will then copy the dropped files to "%LocalAppData%{Random GUID}\", after which the malware will be renamed to bestplacetolive.exe and the original files deleted from the %Temp% directory.

#3

Mimic ransomware consists of multiple threads that employ the CreateThread function for faster encryption and render analysis more challenging for security researchers. When executed, it will first register a hotkey (Ctrl + F1, using the RegisterHotKey API) that displays the status logs being performed by the ransomware. The ransomware's config is located at its overlay and is decrypted using the NOT Operation.

#4

The malware possesses a plethora of capabilities, including the following: Collecting system information, Creating persistence via the RUN key, Bypassing User Account Control (UAC), Disabling Windows Defender, Disabling Windows telemetry, Activating anti-shutdown measures, Activating anti-kill measures, Unmounting Virtual Drives, Terminating processes and services, Disabling sleep mode and shutdown of the system, Removing indicators, Inhibiting System Recovery.

#5

Overall, Mimic ransomware, with its multiple bundled capabilities, seems to implement a new approach to speeding up its routine by combining multiple running threads and abusing Everything's APIs for its encryption (minimizing resource usage, therefore resulting in more efficient execution). Furthermore, the threat actor behind Mimic seems to be resourceful and technically adept, using a leaked ransomware builder to capitalize on its various features, and even improve on it for more effective attacks.

Recommendations

Security Leaders

Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.
- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0009 Collection	TA0011 Command and Control	TA0040 Impact
T1082 System Information Discovery	T1059 Command and Scripting Interpreter	T1129 Shared Modules	T1569 System Services
T1569.002 Service Execution	T1574 Hijack Execution Flow	T1574.002 DLL Side-Loading	T1543 Create or Modify System Process

T1543.003 Windows Service	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1055** Process Injection
T1134 Access Token Manipulation	**T1548** Abuse Elevation Control Mechanism	**T1548.002** Bypass User Account Control	**T1027** Obfuscated Files or Information
T1027.002 Software Packing	**T1070** Indicator Removal	**T1070.001** Clear Windows Event Logs	**T1070.006** Timestomp
T1112 Modify Registry	**T1140** Deobfuscate/Decode Files or Information	**T1222** File and Directory Permissions Modification	**T1007** System Service Discovery
T1012 Query Registry	**T1033** System Owner/User Discovery	**T1057** Process Discovery	**T1083** File and Directory Discovery
T1087 Account Discovery	**T1135** Network Share Discovery	**T1518** Software Discovery	**T1213** Data from Information Repositories
T1489 Service Stop	**T1490** Inhibit System Recovery		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	08f8ae7f25949a742c7896cb76e37fb88c6a7a32398693ec6c2b3d9b488114be 9c16211296f88e12538792124b62eb00830d0961e9ab24b825edb61bda8f564f e67d3682910cf1e7ece356860179ada8e847637a86c1e5f6898c48c956f04590 c634378691a675acbf57e611b220e676eb19aa190f617c41a56f43ac48ae14c7 c71ce482cf50d59c92cfb1eae560711d47600541b2835182d6e46e0de302ca6c 7ae4c5caf6cda7fa8862f64a74bd7f821b50d855d6403bde7bcbd7398b2c7d99 a1eeeeae0eb365ff9a00717846c4806785d55ed20f3f5cbf71cf6710d7913c51

TYPE	VALUE
SHA256	b0c75e92e1fe98715f90b29475de998d0c8c50ca80ce1c141fc09d10a7b8e7ee 1dea642abe3e27fd91c3db4e0293fb1f7510e14aed73e4ea36bf7299fd8e6506 4a6f8bf2b989fa60daa6c720b2d388651dd8e4c60d0be04aaed4de0c3c064c8f b68f469ed8d9deea15af325efc1a56ca8cb5c2b42f2423837a51160456ce0db5 bb28adc32ff1b9dcfaac6b7017b4896d2807b48080f9e6720afde3f89d69676c bf6fa9b06115a8a4ff3982427ddc12215bd1a3d759ac84895b5fb66eaa568bff ed6cf30ee11b169a65c2a27c4178c5a07ff3515daa339033bf83041faa6f49c1 480fb2f6bcb1f394dc171ecbce88b9fa64df1491ec65859ee108f2e787b26e03 30f2fe10229863c57d9aab97ec8b7a157ad3ff9ab0b2110bbb4859694b56923f 2e96b55980a827011a7e0784ab95dcee53958a1bb19f5397080a434041bbeeea 136d05b5132adafc4c7616cd6902700de59f3f326c6931eb6b2f3b1f458c7457 c576f7f55c4c0304b290b15e70a638b037df15c69577cd6263329c73416e490e

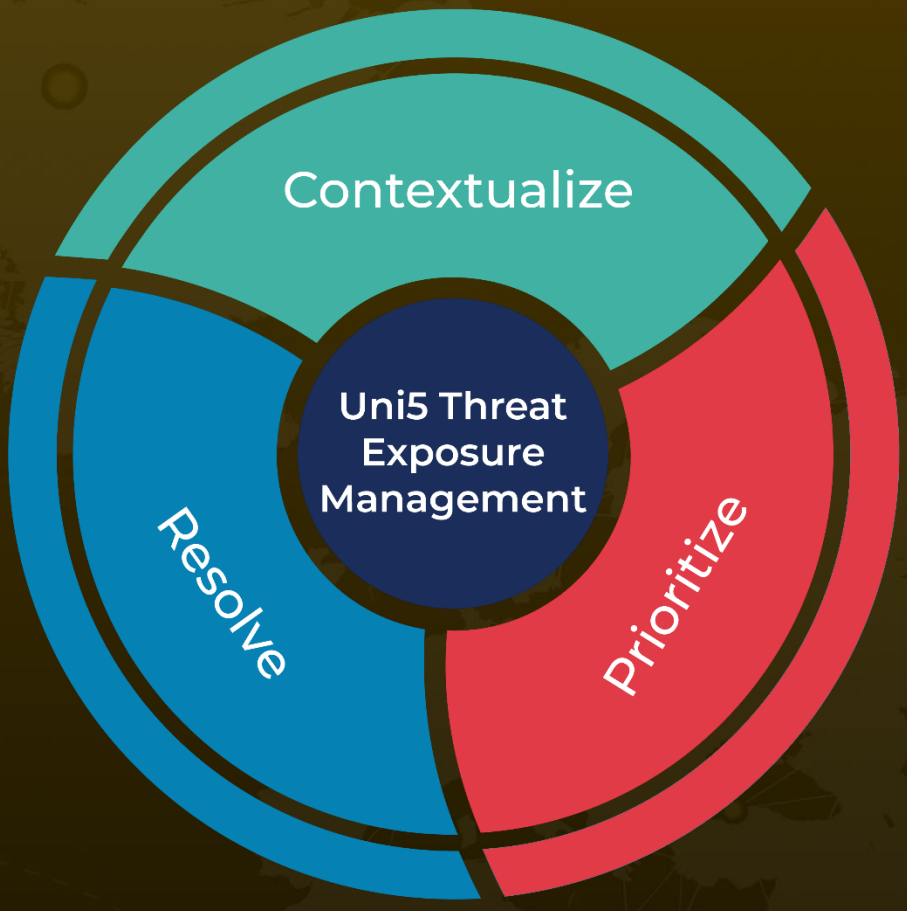
References

https://www.trendmicro.com/en_us/research/23/a/new-mimic-ransomware-abuses-everything-apis-for-its-encryption-p.html

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

January 27, 2023 • 4:11 AM

More at www.hivepro.com