Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

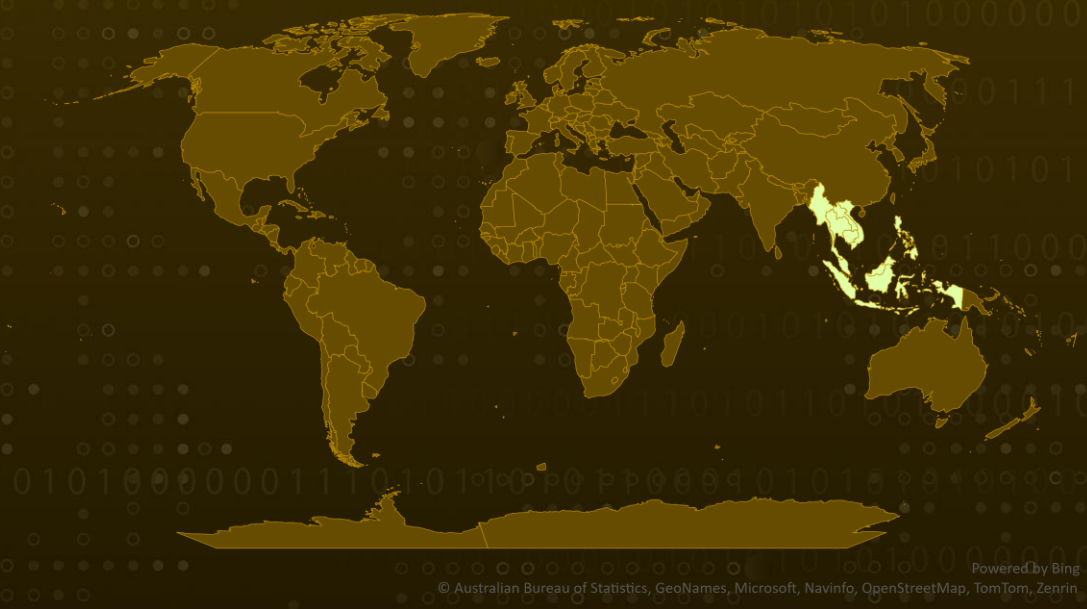
The Intricate Evolution of SoulSearcher Loader for Multi-Stage Malware Execution

Date of Publication	Admiralty Code	TA Number
February 21, 2023	A1	TA2023091

Summary

First appeared: October 2017
Attack Region: Southeast Asia
Attack: SoulSearcher is a type of second-stage loader used by the Soul malware framework, responsible for executing the Soul module payload and parsing its configuration, with multiple variants found in the wild since 2017.

Attack Regions



Attack Details

#1 SoulSearcher is a second-stage loader that has been seen in the wild since October 2017, and it is responsible for executing the Soul module payload and parsing its configuration. The samples found in the wild are all DLLs that follow a similar flow of operation, but with differences in the type and location of the configuration passed to the payload.

#2 SoulSearcher is designed to search for the module and configuration in its overlay data or on the disk. If found, it saves the module to the registry, then fetches the payload from the registry, reflectively loads it, and passes the configuration as an argument. The configuration is decrypted and has the same format as the original Soul backdoor, with an additional field that determines the size of the compressed Soul module in the overlay.

#3 SoulSearcher is a well-crafted loader that shows competent adversarial tradecraft and is a sign of a well-resourced group. Its modular, multi-stage, reflectively executed payloads make it challenging to detect and analyze, and it is likely that the group behind it has more capabilities in their arsenal.

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

TA0043 Reconnaissance	TA0002 Execution	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	T1569 System Services	T1569.002 Service Execution	T1055 Process Injection
T1112 Modify Registry	T1567 Exfiltration Over Web Service	T1041 Exfiltration Over C2 Channel	T1132 Data Encoding
T1082 System Information Discovery	T1083 File and Directory Discovery	T1140 Deobfuscate/Decode Files or Information	T1071 Application Layer Protocol
T1071.001 Web Protocols	T1056 Input Capture	T1056.001 Keylogging	T1059 Command and Scripting Interpreter
T1059.003 Windows Command Shell	T1115 Clipboard Data	T1592 Gather Victim Host Information	T1090 Proxy
T1090.001 Internal Proxy	T1070 Indicator Removal	T1070.006 Timestomp	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	1af5252cadbe8cef16b4d73d4c4886ee9cecddd3625e28a59b59773f5a2a9f7f a6f75af45c331a3fac8d2ce010969f4954e8480cbe9f9ea19ce3c51c44d17e98 c4efb58723fd75d51eb92302fbd7541e4462f438282582b5efa3c6c7685e69fd edb14233eccb5b6e2d731831e7b18b8b17ea6a3f8925fb5899ce2ef985a66b68 fdf0db7f6b60d7563268c15c634adb47e8eec34adfcbf9b10e973916c7517157 c7481d6975646b605aba3fb11686e34ee205f7e280069e9d5bf0c1c2eca79be8

TYPE	VALUE
SHA256	0f7af0cad4aade0e7058051a449059b35358ddda075d88b2d289625adc02deef 3cb4887bec169c75f58bc4ed1c6fd3703cc46512596e62186cf8329448dbb47b cb954f06c94493c87f25651271657aeb1e3e24f26b6552d3e616bbc2dc660679 78feb564c4f6c240ddb17dd0f49ae96df04ee594ed24df81f583136fccf60c1d bc91a4fb16f14fb1c436c2bdc7c80b87a02caa5de17897614d07bc7bda200590 7edd7d406159ab0eecb22ddbd6060de7c24a4eb0b61fa527935310b94d3b9db4 b02b8b6c3d517c6b8652b898963068ba12cd360b5cdcf0aad5fe6ff64f0e9920 ec164902cbe8daaa88ae923719c5dac900715f3e32d4cea6e71ca04c7cecf3e2 bac4b50727c69ca7cc3c0a926bb1b75418a8a0eabd369a4f7118bb9bba880e06 69a9ab243011f95b0a1611f7d3c333eb32aee45e74613a6cddf7bcb19f51c8ab 579fa00bc212a3784d523f8ddd0cfc118f51ca926d8f7ea2eb6e27157ec61260 8ff18b6fb5fe4f221cd1df145a938c57bdd399dc24e1847b0dc84a7b8231458f f97161aaa383e51b2b259bb618862a3a5163e1b8257832a289c72a677adec421 d3647a6670cae4ff413caf9134c7b22b211cb73a172fc1aa6a25b88ff3657597 f5cd13b2402190ec73c526116abea5ebab7bd94bcdb68cc2af4f3b75a69ba9c5 a15eda7c75cf4aa14182c3d44dc492957e9a9569e2d318881e5705da2b882324 967e8063bd9925c2c8dd80d86a6b01deb5af54e44825547a60c48528fb5f896d 64f036f98aad41185163cb328636788a8c6b4e1082ae336dad42b79617e4813d 7b838fcad7a773bfd8bc26a70f986983553d78b4983d0f2002174f5e56f7f521 40fda8137d8464d61240314b6de00ae5c14ed52019e03e4dcadfc00b32c89d23 5dee99beb0b6ba1ebdb64515be1d9307262d9b57b0900310d57290dca40bb427 6b70ad053497f15b0d4b51b5edabeced3077dddb71b28346df7c7ea18c11fcdf 852c98a6fbd489133411848775c19a2525274eac9a89a09a09d511915c7cbafc

TYPE	VALUE
Domains	gmy.cimadlicks[.]net app.tomelife[.]com community.weblives[.]net
IPV4	23.91.108[.]12
Mutex	Global\vQVomit4 Global\mFNXzY0g Global\DefaultModuleMutex Global\DBWinMutex_1 Global\DBWinMutex_2
Event	Global\VirusScanWinMsg Global\3GS7JR4S Global\SecurityEx Global\CacheDataMappingFile
FileName	C:\Windows\System32\wlbsctrl.dll C:\Windows\System32\ikeext2.dll C:\Windows\System32\d6w48ttth.dll C:\Windows\System32\shsvc.dll C:\Windows\System32\netcsvc.dll C:\Windows\System32\fc2qhm7r9.dll C:\Windows\SndVolSSO.DLL SvrLdr_xpsservices.dll timedateapi.dll msfte.dll wsecapi.dll C:\Programdata\Microsoft\svchost.exe NvStreamer.dll Helpsvc32.dll SVCLDR64.dll DataOper64.dll C:\ProgramData\Users.inf %LOCALAPPDATA%\OneDrive\Cache.dat C:\ProgramData\Security_checker\sc.dll C:\ProgramData\Xps viewer\xpsservices.dll C:\Program Files (x86)\CommonFiles\System\ado\msado28.dll C:\ProgramData\networks.dat C:\ProgramData\Microsoft\Crypto\RSA\Keys.dat SntpService.dll sdc-integrity.dat

TYPE	VALUE
Registry	HKCR\.z\OpenWithProgidsEx HKCR\.z\OpenWithListEx HKCR\.sbr\Order HKCR\.sbr\StartOverride HKU\<any_key>\Software\kuhO6Ba0kT HKU\<any_key>\Software\OIfkO2i1 HKU\<any_key>\Software\7QAEGXJc HKCR\.c\Type\Type00 HKR\Software\Microsoft\EventSystem\8C345CCE-5C37-446E-9E36-B57A54FC9C45 HKLM\SYSTEM\CurrentControlSet\Services\<service>\Parameters\8C345CCE-5C37-446E-9E36-B57A54FC9C45 HKR\.kci\PersistentHandler HKCR\.3gp2\Perceived-Type HKCR\.3gp2\Content-Type HKCR\.rat\PersistentHandler\MagicNumber HKCR\.rat\PersistentHandler\TypeFace HKCU\Software\Microsoft\FTP\MostRecentApplication HKCU\Software\Microsoft\FTP\UserInfo HKCU\Software\F32xhfHX

References

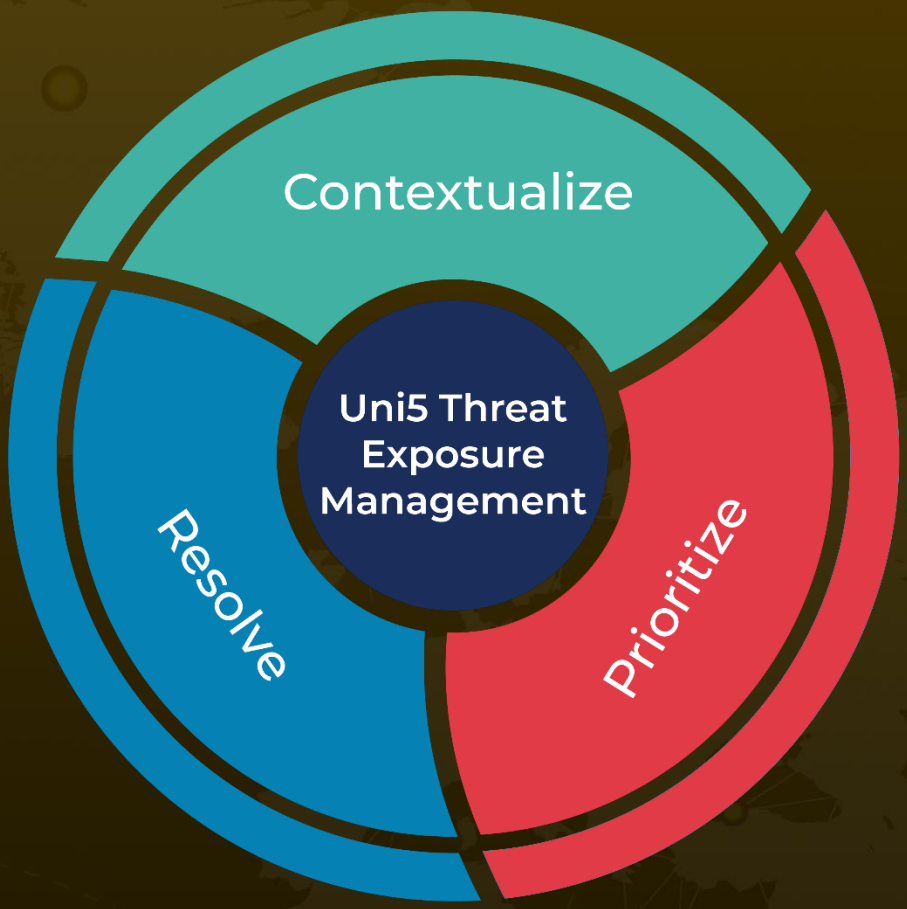
https://www.fortinet.com/blog/threat-research/unraveling-the-evolution-of-the-soul-searcher-malware

https://research.openanalysis.net/yara/soulsearcher/intel/malpedia/worm/2023/02/16/soulsearcher-worm.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

February 21, 2023 • 12:30 AM

More at www.hivepro.com