Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

NetSupport RAT employs phishing campaigns that incorporate Pokemon lures

Date of Publication	Admiralty Code	TA Number
January 18, 2023	A1	TA2023029

Summary

First appeared: 2017
Attack Region: Worldwide
Attack: A version of the NetSupport RAT that has been modified to include malware, giving attackers complete control over the victim's device

Attack Regions

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, OpenStreetMap, TomTom

Attack Details

#1

NetSupport Manager is a remote control tool that can be used by ordinary or corporate users to remotely control systems, but it is being abused by threat actors as it allows external control over specific systems. Unlike RATs, which are mostly based on command lines, remote control tools place emphasis on user-friendliness and offer remote desktops, also known as GUI environments.

#2

Even though they may not have been developed with malicious intent, if they are installed on infected systems, they can be used for malicious purposes by threat actors. The NetSupport RAT malware is being distributed from a phishing page disguised as a Pokemon card game. NetSupport RAT is distributed via spam emails or phishing pages disguised as those for original programs, and is being used by threat actors even in recent days.

#3

NetSupport RAT has been observed in numerous attacks on enterprise environments over the years, and Pokemon is just the latest in a long line of creative lures used to distribute and drop NetSupport RAT.

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

TA0011 Command and Control	TA0002 Execution	TA0003 Persistence	TA0007 Discovery
TA0005 Defense Evasion	TA0004 Privilege Escalation	T1219 Remote Access Software	T1564.001 Hidden Files and Directories
T1047 Windows Management Instrumentation	T1547.001 Registry Run Keys / Startup Folder	T1564.003 Hidden Window	T1036 Masquerading
T1112 Modify Registry	T1406 Obfuscated Files or Information	T1049 System Network Connections Discovery	T1053.005 Scheduled Task
T1053 Scheduled Task/Job	T1083 File and Directory Discovery	T1057 Process Discovery	T1012 Query Registry
T1571 Non-Standard Port	T1547 Boot or Logon Autostart Execution	T1564 Hide Artifacts	T1406.002 Software Packing

Indicators of Compromise (IOCs)

TYPE	VALUE
Domain	she32rn1[.]com
SHA1	593966f38d6b062bec8534ec070a194ac3a3c3d8 3a511941b09fdfed1b53bd89e55be7a3211b19c2 16cf01d8e0753e4b6fac781266d033996af6731d f1c454645ab0adec41765f29861a5b5dd9bda313 0ef99e15452154c240f80c874384d04c46b154a0 ec7e8093b8d35a0e6fbf7b1869d685f0be0e8108 dfc9b696267ae466c6ffa44e63e314df79264afd 4c5771b7fb683b160cb1f7396d39dd706aa7021d

TYPE	VALUE
SHA1	ee3c0579cbcdb5f50ff8cd750a59d89d7757d7a4 288603f501926756c236e368a1fdc7d128f4f9a1 06906aee0ddba30e560e4b60e140e0c098519bb2 7c090065de1090fa92ff01f06739fbca04e6936d 61679dbe1d13d9c25000142fd51b9f4e952a7098 2d6b1900e093c9c8bcce642792e3fadc90b3b0ac 171692daf0a136154edde6e22c791d238ae8c1d0 4233ff7941da62b86fc2c2d92be0572c9ab534c8

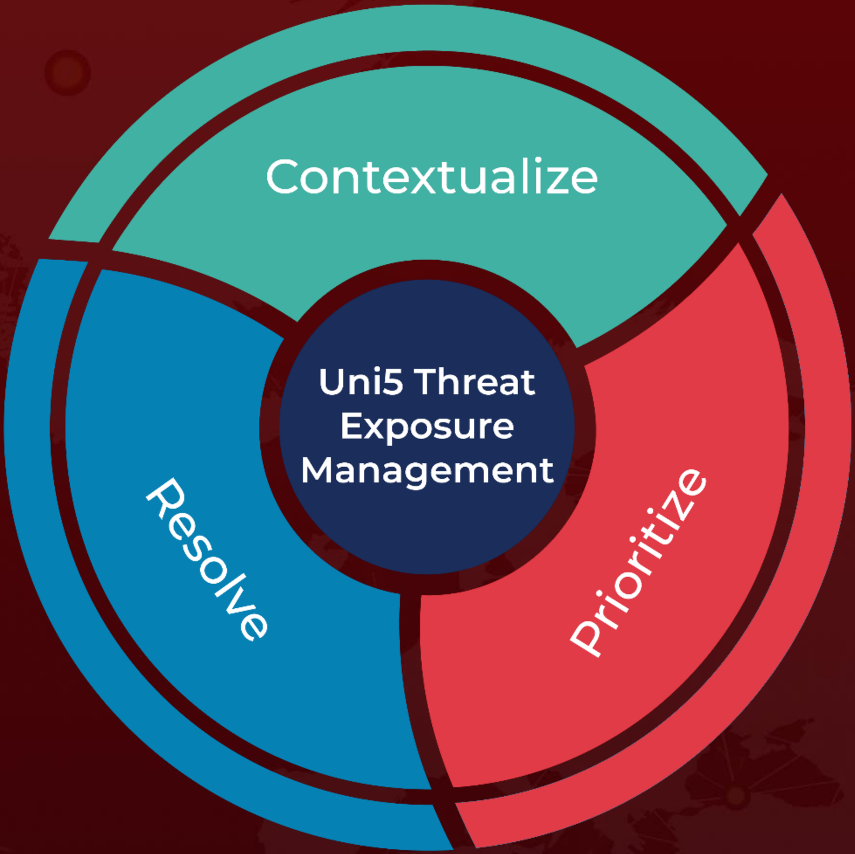
References

https://www.sentinelone.com/blog/gotta-catch-em-all-understanding-the-netsupport-rat-campaigns-hiding-behind-pokemon-lures/

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 18, 2023 • 2:15 AM

More at www.hivepro.com