Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

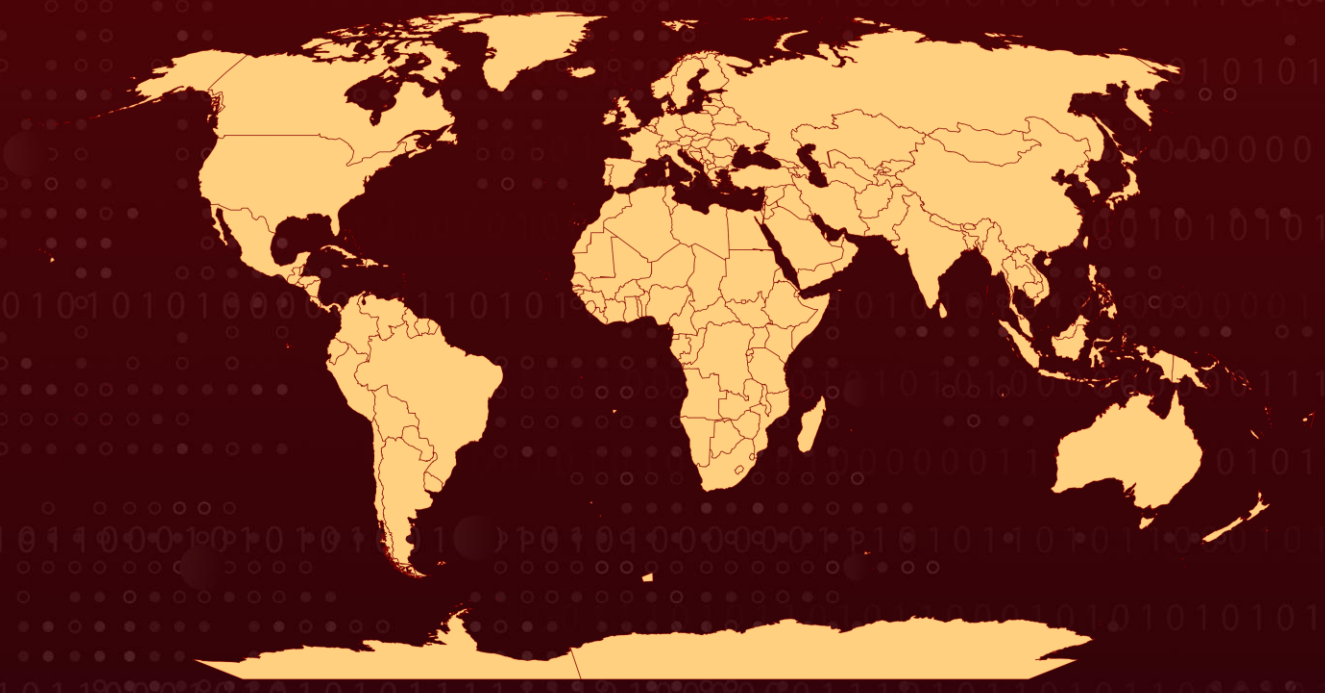
Ice Breaker a Looming Threat on the Gaming Industry

Date of Publication	Admiralty Code	TA Number
February 2, 2023	A1	TA2023059

Summary

First appeared: September 2022
Attack Region: Worldwide
Attack Sector: Gaming and gambling
Attack: Online gaming and gambling companies have been targeted by hackers using unseen backdoors. The attacks are grouped together and referred to as "Ice Breaker." The intrusions make use of smart social engineering strategies to install a JavaScript backdoor.

Attack Regions



Attack Details

#1

The attack sequence proceeds as follows: The attacker poses as a customer and starts a conversation with a gaming company's support agent, claiming to have issues with account registration. The attacker then asks the agent to open a screenshot image hosted on Dropbox. The link provided retrieves an LNK payload or a VBScript file as a backup option.

#2

The LNK file leverages the trusted Windows binary msiexec.exe to download an additional MSI payload from its command-and-control server. During the second stage of the attack, the attacker uses two different payloads. The JavaScript file possesses all the traits of a standard backdoor, enabling the attacker to gather information about running processes, steal passwords and cookies, transfer files, capture screenshots, run VBScripts imported from a remote server, and even set up a reverse proxy on the compromised host.

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

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
T1566 Phishing	T1566.003 Spearphishing via Service	T1204 User Execution	T1204.001 Malicious Link
T1204.002 Malicious File	T1059 Command and Scripting Interpreter	T1059.005 Visual Basic	T1059.007 JavaScript
T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1036 Masquerading	T1036.007 Double File Extension
T1218 System Binary Proxy Execution	T1218.007 Msiexec	T1555 Credentials from Password Stores	T1555.003 Credentials from Web Browsers
T1539 Steal Web Session Cookie	T1057 Process Discovery	T1087 Account Discovery	T1087.001 Local Account
T1518 Software Discovery	T1082 System Information Discovery	T1113 Screen Capture	T1572 Protocol Tunneling
T1571 Non-Standard Port	T1105 Ingress Tool Transfer	T1071 Application Layer Protocol	T1071.001 Web Protocols

Indicator of Compromise (IOCs)

TYPE	VALUE
Domains	screenshotcap[.]com screenshotlite[.]com screenshot[.]icu xn--screnshot-iib[.]net xn--screnshot-jib[.]net ponzix[.]net

TYPE	VALUE
IPV4	178[.]63[.]65[.]51 194[.]5[.]97[.]17
SHA256	a857fbb06f493cd63f2c8128038bf78d1467295e89be0c9848edd8a2dd8b44e8,185182f369edcb96118a91dcad39eb5b63239112ed6963a8c274178bf1b55394,0f043b90f6fa68551221ec560068aac4abb90749ca42a63dd62664e483940ec3,24df9651a38ab5328d59ab1c448a98afb3df8209b8877bbde63d49308e0d8c68,31d03d305354eb92f3ea0420b0f674bf6414422b24bb717ec28dfacdc2647a1d,3b86fb030c0d1b440307b8d2ca7bbe2590d58e5a28118985e9774990a1c74d21,978940d9785d3ade9f1c9b13ce35d67af2f47091740c2a4a5978e512543e6d76,a0a5a12f4781433ef3c0abd89186bd987f5d02c4e643803d92ff0413852d2486,a2047deac9bb8af7107e35b6e3c8617bec01dd9121a76f4fbca1fa8c760ba40e,a6e97bdbd841c9ac8bdad6145cbe65f38a31d74eb9c00346bb5b3a005508b544,aa2521bf540a4070ebf4ad340051d4df1b9608eff22e0110a0a49e1289cdbf03,b8791cc1ec61e61b59cb8c251b49c644a597025fe1d1195e960212980822a93d,f97ee203a3dd08ac38d16295dbf9cb0c7476690ba03a05afefed34d7e8cfd44e,fee0935cec808fe27112cf3c40e91d4702872f43064e9e9f71f9f1e6a8894eaf,9ea31ef8ee5abaae8752f1db783431cbb9e691a457ae2cfe648210adeefb8eff,f3645c8b04fe683ade9b5a46db8af6428c15e94730a25f05bf2378a4b28ad065,8727e8759232721413c038e45c5e05cbfe5194489c060875f273329db2aa7c08,e3a7c1c8b8fe7a2fce89318015187adb672c31747d966218c962c91248179553,b5ab83ceacfa4fba714d515248f166900f1b21e9a946e684be1e415439677309
MD5	c97293c4d10331f9bc47b041c8ce4e0e
SHA1	84d614acc666abb6f95cfc3e432a2ee07faccb69
URLs	hxxps://screėnshot[.]net/Ycp3lI.jpg

References

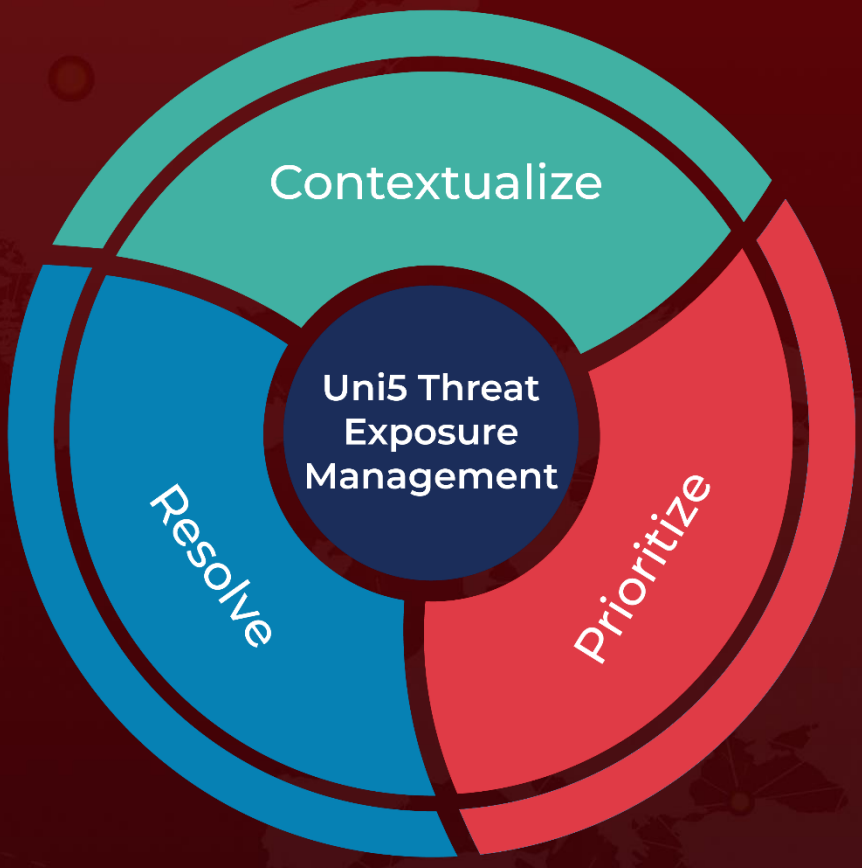
https://www.securityjoes.com/post/operation-ice-breaker-targets-the-gam-bl-ing-industry-right-before-it-s-biggest-gathering

https://www.bleepingcomputer.com/news/security/hackers-use-new-icebreaker-malware-to-breach-gaming-companies/

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 2, 2023 • 3:00 AM

More at www.hivepro.com