Bridewell

Threat Advisory

Undetected North Korean Malware: A Looming Threat to Financial Institutions

Date: 16/02/2023

TLP: WHITE

Summary

Bridewell Intelligence has identified a looming threat to financial institutions related to a cluster of malicious North Korean malware, which is currently unreported and undetected by anti-virus solutions. This information was discovered by pivoting from recent Proofpoint and Kaspersky reporting that revealed activities of TA444, a North Korea state-sponsored threat actor that is financially motivated and actively targeting cryptocurrencies and financial institutes. It is estimated that threats actors related to North Korea stole over $1 billion USD of cryptocurrency assets during 2022 alone.

TA444 has been actively targeting banks for several years, but in the latter stages of 2022, the group expanded its operations to include cryptocurrency. The group has demonstrated a startup mentality, using rapid iteration and the testing of products on the fly. Recently, Proofpoint researchers identified a deviation in TA444's operations, indicating a shift in objectives and highlighting the need for vigilance in the face of evolving threats.

This advisory report aims to provide details of malicious indicators of compromise and mitigation measures for financial institutes and cryptocurrency exchanges to protect themselves against the threat of North Korean malware.

Discovered TA444 Infrastructure

Despite existing research into the impact of TA444 operations, their command-and-control (C2) malware largely remains undetected by conventional solutions and services. Further limited reporting on their tactics and techniques makes defending against the threat even more difficult.

As a result, Bridewell Intelligence is sharing the following indicators to support network defenders.

IP	ISP	VirusTotal Detections*
155[.]138.159.45 *(Reported by Kaspersky on Dec 2022)*	Vultr	5/88
104[.]255.172.56	H4Y Technologies	0/88
172[.]93.181.221	Router Hosting	0/88
172[.]86.123.181	Router Hosting	0/87
172[.]86.122.181	Router Hosting	4/88

**Out of the five detected IPs, one has been previously reported by Kaspersky in December 2022 and three of the five IPs have zero detections out of 88 anti-virus vendors.*

Further Indicator Analysis

TA444 is a highly skilled and sophisticated threat group that has been known to use multiple tactics to avoid detection and carry out their malicious activities. Among their tactics, they have been observed to favour the use of both Porkbun DNS servers and Cloudflare services.

By using Porkbun DNS servers, they are able to obscure their activities and evade detection by security tools that rely on domain blacklists. In addition, they often leverage Cloudflare services to mask their true IP address and make it more difficult for defenders to track and locate their operations.

Intelligence Assessment

Early detection of C2 malware is critical to prevent the ability to progress the attack further within the victim network. Organisations can leverage the expertise of security vendors to identify undetected malware that may have already infiltrated their systems through the integration of Threat Intelligence into their detection and hunting capabilities.

As above, the tactics deployed by TA444 can make it challenging for security teams to detect and respond to their activities. Organisations should consider implementing security measures, such as a Managed Detection and Response (MDR) service that integrates timely intelligence, to detect and respond to threats from TA444 and other advanced threat groups. It's also important to stay current on the latest threat intelligence to better understand the tactics and techniques used by these groups.

Bridewell Intelligence advises individuals and organisations to remain vigilant by adopting robust security measures, staying informed about the latest developments in cryptocurrency-related threats, and seeking expert guidance to ensure that their assets remain safe and secure.

Financial institutions, in particular, should be especially cautious and proactive in implementing measures to detect and prevent attacks from TA444 C2 severs, given the potential for significant financial losses. It is crucial to recognise the threat and take action to prevent becoming a victim.

Bridewell Intelligence will continue to monitor the situation and provide updates as needed to help individuals and organisations stay informed and protected against this and other emerging threats.

Mitigations

It is recommended for organisations to conduct a retrospective search in their environment for any connection attempts to the listed indicators discovered and published by Bridewell.

Additionally, organisations should add these indicators to a reference set with alerting, in the event of any attempted connections or add to an active block list.

Bridewell Intelligence also recommends the following additional measures:

1. Implement Network Segmentation: Divide the network into smaller, isolated subnetworks to limit the potential impact of a security breach by isolating traffic to and from C2 servers.
2. Deploy Advanced Threat Detection Systems: Use advanced threat detection systems that use machine learning algorithms to identify and block any suspicious traffic.
3. Conduct Regular Security Audits: Regular security audits help detect vulnerabilities and potential security gaps and ensure that all systems and applications are up-to-date with the latest security patches.
4. Limit Access to Sensitive Data: Ensure that only authorised personnel have access to sensitive data and use multi-factor authentication (MFA) to add an extra layer of security.
5. Employee Security Training: Educate employees on best security practices, such as the importance of strong passwords and how to identify and report potential security threats.
6. Implement Effective Incident Response Plan: Have an effective incident response plan to identify, contain, and mitigate potential security incidents.

By following these measures, organisations can effectively process indicators related to C2 servers and malicious infrastructure and prevent potential cyberattacks. It is important to continuously monitor logs and remain vigilant to evolving security threats, and adding MFA can further enhance the security of sensitive data.

How Bridewell Helps its Clients Stay Secure

Bridewell works with its clients to effectively manage cybersecurity risks, with the following key practices:

- Cyber Threat Intelligence: Bridewell customers subscribe to the cyber threat intelligence service to stay updated on the latest threats and vulnerabilities. Bridewell has a dedicated team to analyse the latest intelligence and prioritise the threats based on their potential impact to the client's organisation.

- Vulnerability Management Program: Bridewell provides a comprehensive vulnerability management program to identify, assess, and mitigate potential vulnerabilities for its customer's networks, systems, and applications. The program includes regular vulnerability scanning, penetration testing, and patch management.

- Active 24/7 Managed Detection and Response: Bridewell customers benefit from a dedicated Security Operations Centre (SOC) which provides 24/7 monitoring of the company's IT and OT systems. The SOC uses advanced threat detection tools and techniques to identify, investigate, and respond to potential threats in real-time.

The key benefit for Bridewell customers is that the different services work in tandem.

The threat intelligence team inform the vulnerability management of new and emerging threats that may affect the organisation. The vulnerability management team prioritise the most critical vulnerabilities to address, based on the potential impact of a successful attack.

The SOC actively monitor the networks and systems to identify and respond to potential threats, using the insights provided by the vulnerability management team and threat intelligence to identify activity based upon indicators and behaviours.

By following these practices, Bridewell customers take a proactive approach to cybersecurity and are better protected against the constantly evolving threat landscape.

Conclusion

Bridewell Intelligence has identified a significant threat to financial institutions related to North Korean malware that is currently undetected by anti-virus solutions. This threat is a result of the activities of TA444, a North Korean state-sponsored threat actor that has expanded its operations to include cryptocurrency and is financially motivated.

Bridewell Intelligence has provided indicators of compromise and recommended mitigation measures for financial institutions and cryptocurrency exchanges to protect themselves against this threat.

Contact and Feedback

We intend to provide clear, concise, and actionable advice on key cyber security vulnerabilities, exploits and incidents. Was this advisory valuable to your organisation? Your comments and feedback are important to us. Feedback can be returned to cyberthreatintelligence@bridewell.com.

References

Name	Link
ProofPoint TA444 report Jan 2023	https://www.proofpoint.com/uk/blog/threat-insight/ta444-apt-startup-aimed-at-your-funds
BlueNoroff introduces new methods bypassing MoTW Dec 2022	https://securelist.com/bluenoroff-methods-bypass-motw/108383/

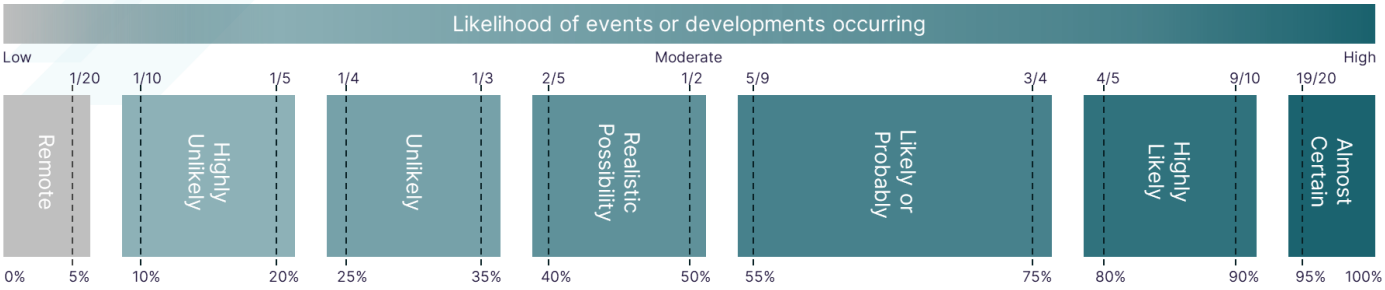
Appendices

Domain	IP	DNS Server	VirusTotal Detections
site[.]siteshare.me	155[.]138.159.45	Porkbun.com	0/87
one[.]microshare.cloud		Porkbun.com	13/88
doc[.]gdocshare.one		Porkbun.com	14/88
dmarc[.]onlineshares.cloud		Porkbun.com	0/87
_dmarc[.]onlineshares.cloud		Porkbun.com	0/87
www[.]onlineshares.cloud		Porkbun.com	0/87
ms[.]msteam.biz		Porkbun.com	14/88
open[.]onlinecloud.cloud		Porkbun.com	13/88
www[.]onlinecloud.cloud		Porkbun.com	12/88
fs[.]digiboxes.us		Porkbun.com	13/88
www[.]docuprivacy.com		Porkbun.com	1/88
team[.]msteam.biz		Porkbun.com	14/88
ms[.]onlineshares.cloud		Porkbun.com	14/88
www[.]privacysign.org		Porkbun.com	12/88
share[.]1drvmicrosoft.com		Porkbun.com	14/88
ns1[.]trytiponlineresult.com		registrar-servers.com	0/87
ns2[.]trytiponlineresult.com		registrar-servers.com	0/87
trytiponlineresult[.]com		registrar-servers.com	1/88
shippingspro[.]com		TopDNS	0/88
corporateimageguru[.]com		Hostgator	0/88
naogoze[.]com		Parked	0/88
www[.]naogoze.com		Parked	0/88
phcnetworks[.]net		Cloudflare.com	0/88
server-1[.]phcnetworks.net		Cloudflare.com	0/88
www[.]phcdevworks[.]com		Cloudflare.com	0/88
phcdevworks[.]com		Cloudflare.com	0/88
cloud[.]mekongcapital.net	104[.].255.172.56	registrar-servers.com	1/88
cloud[.]j-ic.com		namecheaphosting.com	0/88
down[.]tomming.us		registrar-servers.com	0/88
cloud[.]gpmtreit.co		namecheaphosting.com	1/88
cloud[.]espcapital[.]pro		namecheaphosting.com	10/88
cloud[.]j-ic[.]co		registrar-servers.com	1/88
nbright[.]best		registrar-servers.com	0/88
down[.]espcapital.co		namecheaphosting.com	0/88
internal[.]j-ic.co		registrar-servers.com	1/88
down[.]j-ic.co		registrar-servers.com	0/88
down[.]gpmtreit.us		registrar-servers.com	0/88
down[.]gpmtreit.co		namecheaphosting.com	0/88
down[.]j-ic.com		namecheaphosting.com	0/88
tet[.]dnx.capital		namecheaphosting.com	6/88
cloud[.]dnx.capital		namecheaphosting.com	6/88
cloud[.]azurehosting.co		Parked	0/88
cloud[.]anobaka.info		Parked	6/88
docs[.]azurehosting.co		Parked	4/88
share[.]anobaka.info		Parked	15/88
safe[.]doc-share.pro		dnsowl.com	0/87
safe[.]doc-share.top		dnsowl.com	0/87
autoprotect[.]com.de		centralnic.net	4/88

autoprotect[.]gb.net	172[.]93.181.221	centralnic.net	2/88
autoprotect[.]com.se		centralnic.net	0/88
safe[.]doc-share.cloud		dnsowl.com	8/88
nbright[.]best		registrar-servers.com	0/88
www[.]hoststudio.org	172[.]86.123.181	Porkbun.com	0/87
www[.]updatezone.org	172[.]86.122.181	Porkbun.com	9/88
www[.]thecloudnet.org		Porkbun.com	13/88

Probability Yardstick

Threat assessments and reporting will generally provide some indication as to the likelihood of a threat actor attempting to target you, your organisation or your sector, or the tactics, techniques, and procedures used to perform an attack. Such assessments will often use probabilistic language the yardstick, as below, gives general probabilities associated with the language used. This provides a central professional standard for government intelligence assessment to reduce uncertainty around the use of probabilistic language.



Traffic Light Protocol

Traffic Light Protocol (TLP) is used to ensure that intelligence is shared with those who it will have the most impact with. There are four levels to the TLP. They work in similar ways to the document marking scheme.

TLP RED – Not for disclosure, restricted to the client or participants only.

TLP AMBER – Limited disclosure restricted to the clients or participants'

TLP GREEN – Limited disclosure, restricted to the client or community.

TLP WHITE – Disclosure is not limited.

+44 (0)3303 110 940
cyberthreatintelligence@bridewell.com
bridewell.com

Bridewell