Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

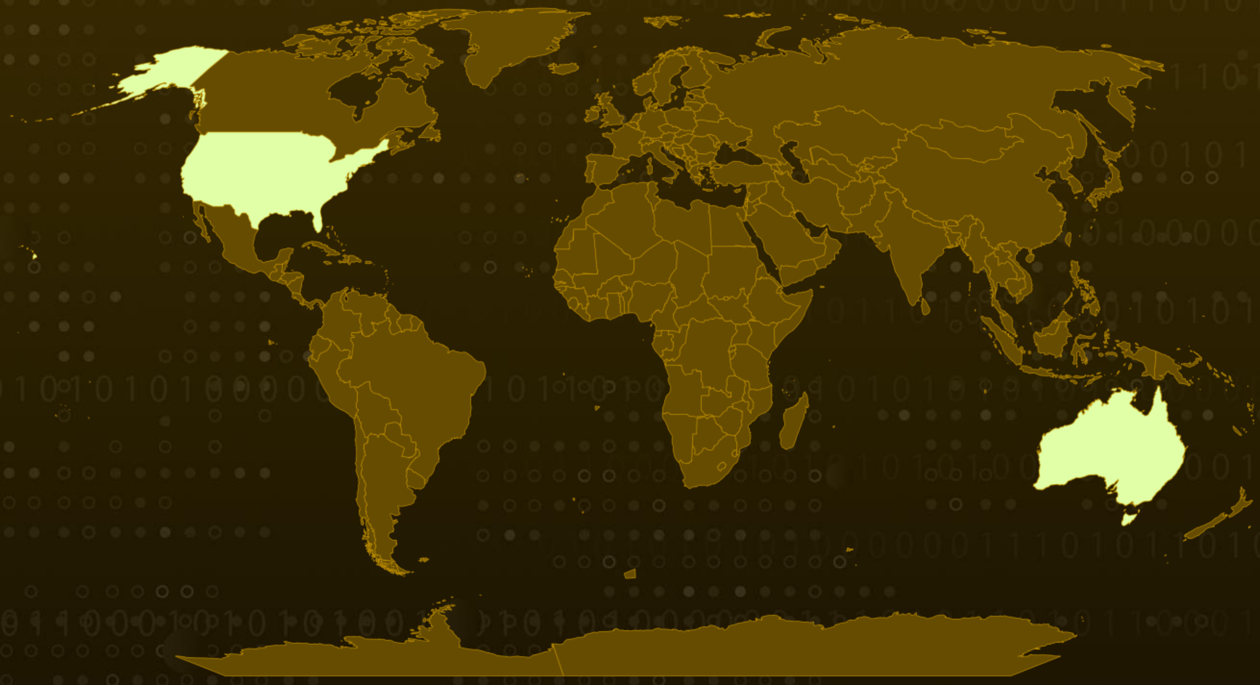
Tracing the Footprints of Agent Tesla's Conspirators

Date of Publication	Admiralty Code	TA Number
April 4, 2024	A1	TA2024129

Summary

Attack Commenced: November 2023
Malware: Agent Tesla
Attack Region: Australia and USA
Attack: The Agent Tesla malware, classified as a remote access trojan (RAT), demonstrates remarkable proficiency in infiltrating systems to extract sensitive information like keystrokes and login credentials from web browsers and email clients. It is primarily spread through phishing campaigns, with a specific focus on obtaining organizational email credentials. This facilitates unauthorized access for further malicious activities.

Attack Regions



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

Attack Details

#1 The Agent Tesla malware operates as a remote access trojan (RAT), proficient in extracting and infiltrating sensitive data from compromised systems. This malicious software is capable of harvesting a wide range of information, such as keystrokes and login credentials used in web browsers and email clients on infected devices.

#2 Primarily distributed through phishing campaigns, the malware targets organizational email credentials, enabling access to targeted entities for further illicit activities. A recent instance of Agent Tesla's operations focused on American and Australian organizations.

#3 Two cybercrime actors are implicated in orchestrating these operations: Bignosa, the primary figure associated with a collective involved in malware and phishing endeavors, primarily targeting entities in the USA and Australia, as well as individuals.

#4 Operating under a dual persona, "Gods," also known online as "Kmarshal," transitioned from prior involvement in phishing attacks to orchestrating malware campaigns. Upon interaction with a malicious email, recipients unknowingly download and execute the Agent Tesla sample, fortified by the Cassandra Protector.

#5 Tailored to interact exclusively with .NET samples, this protector incorporates various features, including anti-AV and anti-emulation mechanisms. Observations suggest that the actors communicate via Jabber, utilizing this service for instant messaging through an open protocol.

Recommendations

Monitor Network Traffic and Communication Channels: Implement network monitoring tools to detect unusual or suspicious activities, such as communication with known command and control servers associated with Agent Tesla. Monitor communication channels like Jabber for signs of malicious activity.

Continuous Monitoring and Analysis: Implement continuous monitoring and analysis of network traffic and system logs. This proactive approach can help identify anomalies and potential threats before they escalate.

Disable Unnecessary Services: Review and disable unnecessary services and features on systems to minimize potential attack vectors. Restrict user privileges to limit the impact of potential breaches.

Heighten Awareness: Familiarize yourself with common social engineering tactics and deceptive strategies employed by threat actors. Knowing the signs of malicious activity can help you avoid falling victim to scams.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0002** Execution	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0011** Command and Control	**TA0010** Exfiltration	**T1041** Exfiltration Over C2 Channel
T1056 Input Capture	**T1027** Obfuscated Files or Information	**T1049** System Network Connections Discovery	**T1059** Command and Scripting Interpreter
T1021 Remote Services	**T1566** Phishing	**T1212** Exploitation for Credential Access	**T1071** Application Layer Protocol
T1005 Data from Local System	**T1566.001** Spearphishing Attachment	**T1555.003** Credentials from Web Browsers	**T1555** Credentials from Password Stores

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	105[.]160[.]122[.]192, 105[.]161[.]75[.]138, 105[.]161[.]81[.]79, 197[.]237[.]92[.]228, 41[.]90[.]176[.]165, 41[.]90[.]177[.]10, 41[.]90[.]179[.]140, 41[.]90[.]180[.]123, 41[.]90[.]180[.]219, 41[.]90[.]181[.]104, 41[.]90[.]185[.]44, 41[.]90[.]186[.]173, 41[.]90[.]186[.]247, 41[.]90[.]186[.]248, 41[.]90[.]188[.]113, 41[.]90[.]189[.]214, 91[.]215[.]152[.]7, 147[.]189[.]161[.]184, 149[.]0[.]216[.]243, 149[.]0[.]91[.]214, 176[.]218[.]220[.]145, 192[.]223[.]25[.]77, 192[.]223[.]25[.]85, 212[.]133[.]214[.]104, 31[.]155[.]119[.]217, 46[.]2[.]179[.]191, 46[.]2[.]181[.]103, 46[.]2[.]254[.]164, 46[.]2[.]35[.]156, 79[.]110[.]48[.]6, 84[.]38[.]130[.]226, 91[.]92[.]244[.]255, 142[.]202[.]188[.]238, 156[.]227[.]0[.]187, 45[.]38[.]135[.]112, 80[.]68[.]159[.]15, 91[.]210[.]166[.]29, 142[.]202[.]190[.]222, 172[.]81[.]60[.]206, 192[.]236[.]146[.]12, 192[.]236[.]194[.]247, 192[.]236[.]236[.]35

TYPE	VALUE
Email	admin[@]dllserver[.]top, andrewbailey[@]sent[.]com, baileyandrewjr[@]mailo[.]com, contact[@]chserver[.]top, dickson[@]outlook[.]com, enquires[@]dllserver[.]top, felixjensen84[@]gmail[.]com, felixjensenjr[@]gmail[.]com, felixreederjr[@]gmail[.]com, iamhere[@]mailo[.]com, info[@]chserver[.]top, info[@]sterdiffa-wat[.]site, iwork[@]hot-chilli[.]net, lwork6356[@]gmail[.]com, nosakharegodson[@]gmail[.]com, peterdave[@]mailo[.]com, peterdavejr[@]gmail[.]com, peterdavejr[@]mailo[.]com, sales[@]kenyapride[.]co[.]ke, support[@]chserver[.]top, support[@]cloverleave[.]info, support[@]dllserver[.]top, support[@]sterdiffa-wat[.]site, account-security[@]eutrade[.]top, dfk[@]dtdc[.]eu[.]org, gods[@]openim[.]eu, info[@]eutrade[.]top, j[.]klaus[@]johnokimattorney[.]eu[.]org, kmarshal101[@]hotmail[.]com, kmarshal[@]jabbers[.]one, kmarshal[@]sure[.]im, legal[@]johnokimattorney[.]eu[.]org, logteam101[@]gmail[.]com, logteam[@]netc[.]eu, msgate[@]net-c[.]ca, no-replu[@]hlgroup[.]eu[.]org, no-reply[@]hlgroup[.]eu[.]org, noreply[@]grillminings[.]tech, onye[.]oma50[@]gmail[.]com, smtps[@]hlgroup[.]eu[.]org, unlimitedsendertech[@]gmail[.]com

TYPE	VALUE
SHA256	8ba55cc754638714764780542eefd629c55703ecf63ae20d5eb65b8c14d3e645, 87709f72683c5ffc166f348212b37aadb7943b5653419f2f0edf694fb50f1878, 691761d401a6650872d724c30b7ef5972e3792e9a2ba88fdca98b4312fb318d8

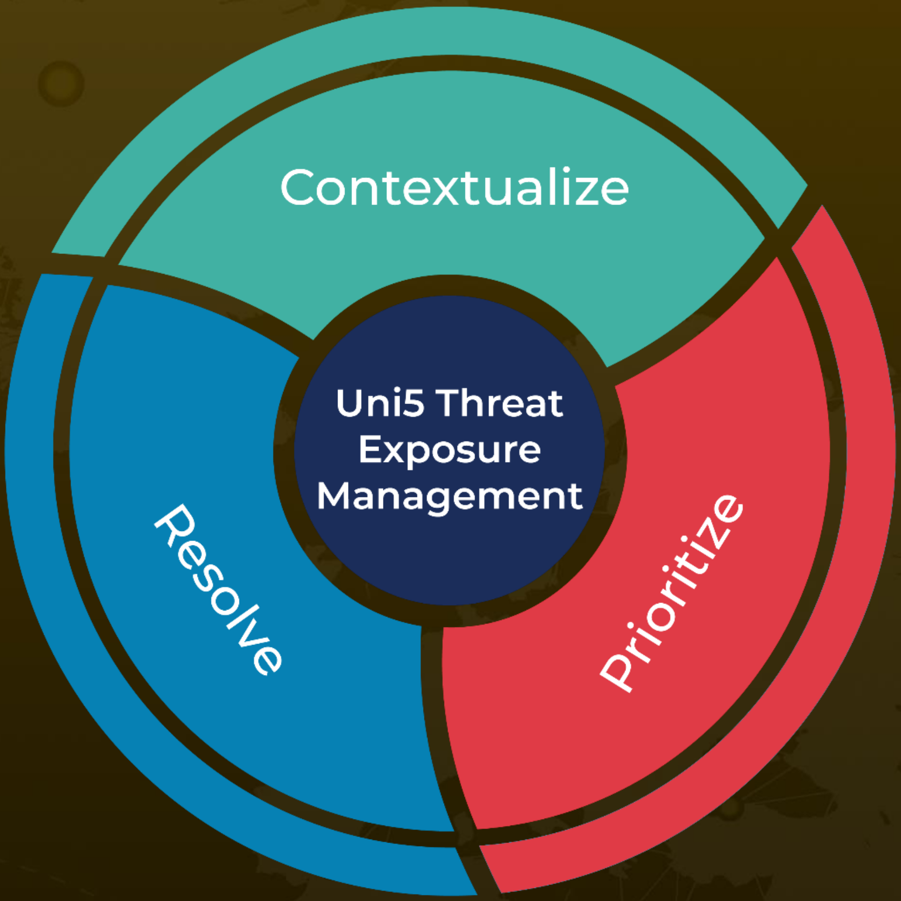
References

https://research.checkpoint.com/2024/agent-tesla-targeting-united-states-and-australia/

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

April 4, 2024 • 5:00 AM

More at www.hivepro.com