Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

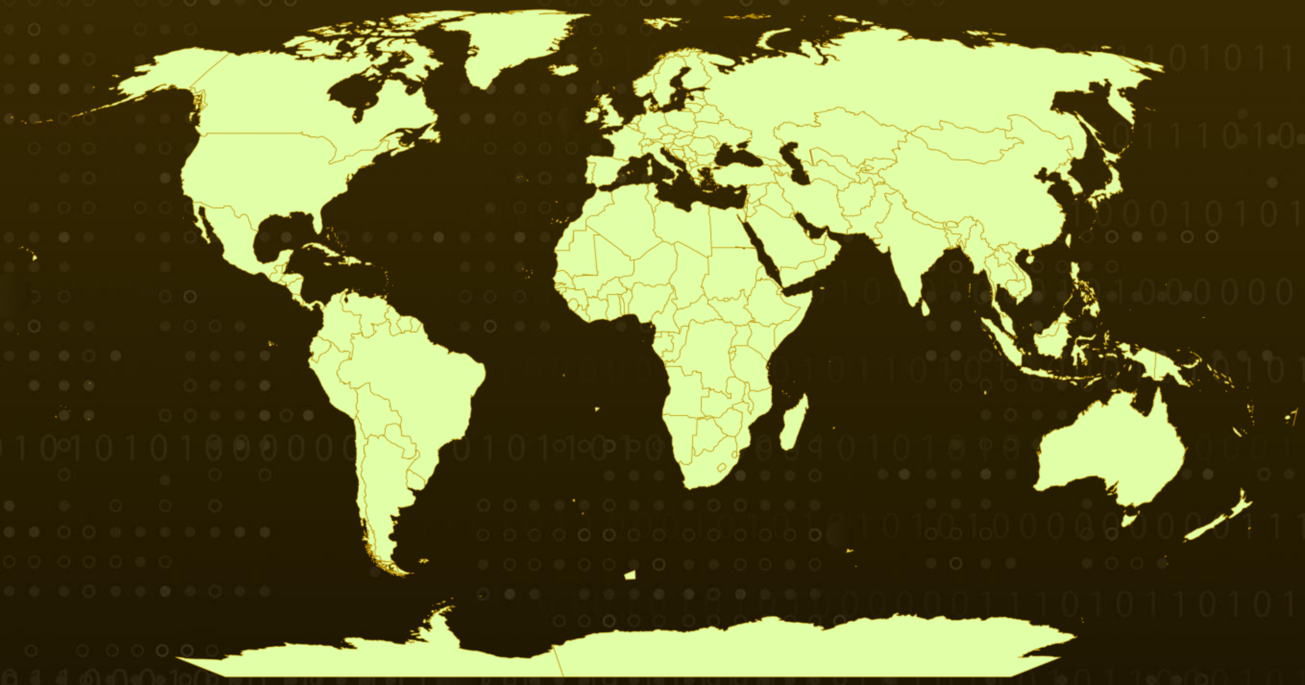
From Observer to Asuka - The Reinvention of Stealer

Date of Publication	Admiralty Code	TA Number
March 21, 2024	A1	TA2024111

Summary

First Appearance: May 2023
Malware: AsukaStealer
Attack Region: Worldwide
Attack: A malware-as-a-service (MaaS) called 'AsukaStealer,' advertised on a Russian-language cybercrime forum by the alias 'breakcore,' has surfaced. Priced at $80 per month, AsukaStealer is written in C++ and features customizable configurations and a user-friendly interface designed for harvesting data.

Attack Regions



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

Attack Details

#1 A malware-as-a-service (MaaS) known as 'AsukaStealer,' promoted on a Russian-language cybercrime forum under the alias 'breakcore,' has been uncovered. The perpetrator advertises its availability for $80 per month.

#2 AsukaStealer, crafted in C++, boasts adaptable configurations and a user-friendly web-based interface, designed to harvest data from various sources including browsers, extensions, Discord tokens, FileZilla and Telegram sessions, cryptocurrency wallets, desktop screenshots, and files from the Steam Desktop Authenticator application.

#3 It is worth noting that 'breakcore' previously operated under the name 'ObserverStealer,' selling their creation on hacking forums until July 2023, albeit with limited success. AsukaStealer appears to be a reimagined version of ObserverStealer, with likely refinements made to enhance its appeal to cyber criminals.

#4 AsukaStealer's binary code reveals conspicuous elements such as base64-encoded and hexadecimal values. Employing XOR encryption for its command and control (C2) addresses, AsukaStealer funnels logs through a singular C2 address by default, although clients have the option to configure custom proxies.

#5 Proficient threat actors skilled in malware development and equipped to maintain substantial command and control infrastructure continue to exploit opportunities to sell malware-as-a-service (MaaS), catering to clandestine communities while reaping rapid financial gains. The emergence of AsukaStealer underscores the ongoing trend of information-extraction malware proliferating as MaaS offerings within the Russian cybercrime ecosystem this year.

Recommendations

Endpoint Protection: Implement robust endpoint protection solutions with features such as real-time threat detection, sandboxing, and endpoint detection and response (EDR) capabilities to safeguard endpoints from malware infections.

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

TA0001 Initial Access	**TA0002** Execution	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0007 Discovery	**TA0009** Collection	**TA0011** Command and Control	**TA0010** Exfiltration
T1003 OS Credential Dumping	**T1056** Input Capture	**T1555.003** Credentials from Web Browsers	**T1528** Steal Application Access Token
T1539 Steal Web Session Cookie	**T1018** Remote System Discovery	**T1083** File and Directory Discovery	**T1082** System Information Discovery
T1518.001 Security Software Discovery	**T1005** Data from Local System	**T1119** Automated Collection	**T1113** Screen Capture
T1176 Browser Extensions	**T1041** Exfiltration Over C2 Channel	**T1140** Deobfuscate/Decode Files or Information	**T1212** Exploitation for Credential Access

Indicators of Compromise (IOCs)

TYPE	VALUE
URL	hxxp[://]5.42.66[.]25/
IPv4	5[.]42[.]66[.]25
Domains	www.simplyavailable[.]com, freemsk[.]org
MD5	2d2b66d90495c1236f2e557172bf0f1c, 7ce0bd101d349bc88b668e380093e1a9, e9dda8ccde5385e8d0a7f0bdc361e51d, 28b7d6b0a793d772c953f529742ca91f, 9ce2a046a0698212c2963f2df91ff2e1, 20017810fba85ef8ac6e4230d0e67a07, 371e14f7e146ff22cb9ebe2f78cbfb7f, 1494c8bc32576cb008c33d6f0fd1e842, 75c79796fa147bf3f4d569b544ee0547, 2de37ffcae86c673de3cd2ee5e2ad3b1
SHA1	a06d203ae9cbe26a3c2e389f1c361ac49ef54c08, 45fc72df60f39ebe77d4012f34a10e73eb2fd485, 863734caf0cb94dce610fe49eeebe438a7096dfb, fc33fe3deb280d9ed94e3add58134660433bdb18, 69a2d82f13246761e6d5159efb78b8fa91856380, d7b6530a4c7d685e9ee6765231bab14fecdadeba, 2fde663b31a46e83f3034464674ad3f3a85f6972, 4b3cdfbeaa9f8dc3554a0f9a54fc0d16334a46ed, 5c6a4cd4b9271410cc45ccda00a2531631f35136, 09f2187f0228eed3df41c76c69d94da789c0f2f1
SHA256	24bb4fc117aa57fd170e878263973a392d094c94d3a5f651fad7528d5d73b58a, 00cc1ef3d307750d5cdbe537da606101e90091b6020c71f696e454aee11c9a98, 5b2b8a4d5b8375a3ac2ce68b93cdbfdc8fd13d1cf4ea1a6a61bd784aa495dbfb, 5f2016f22935cea6fa5eafe1e185d6a9b4c14c4b2aa8619ec15a539358cac928, 6b0e95d68da6d029a4af645a408c0608218e853f11c8ba70a14b06ec2a005424, 9ac629ed8e07b6c99b05edd46b86e1795e5f96908ab1fe85a06282b0a982cd1b, bb17d47f10fefcee4c883f93f2989e753b969298dd70262ae00696dd482dc9b4,

TYPE	VALUE
SHA256	c534f184b8ea3887161ec2b364de15e61ee9a4053f8902450383d3f4165fc818, dc723d302340d27529b8c3c880b4cf53534a02e2a71a68f39eec30f239c2c988, e6430183aa7bbaffa89ffbef7bfac3aa54481e904556ab71ea20ccf55dfce53f, 0e5470a33fd87b813ecf72370f9e1f491515c12f41c8ea3c7bbc169ac56acda5, 476171dd2eb7f118d3e0aff32b7264d261ba4c2d9fa6c14ccff6d8d99b383db4

References

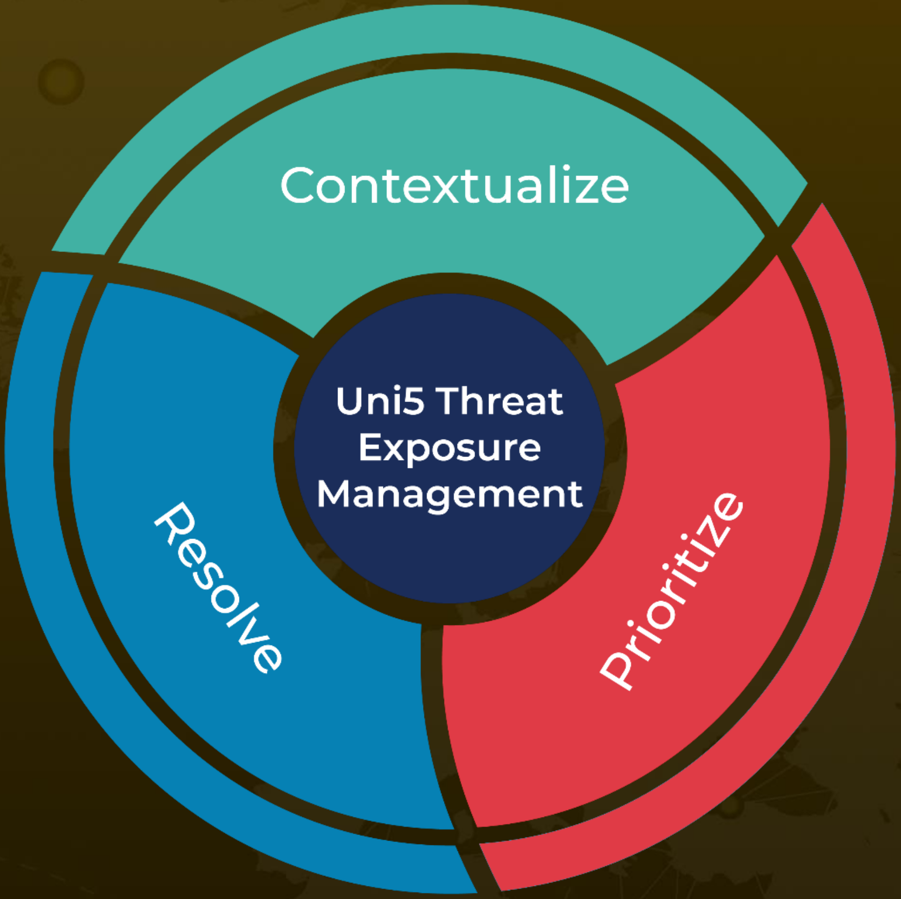
https://any.run/cybersecurity-blog/asukastealer-malware-analysis/

https://cyble.com/blog/asukastealer-a-revamped-version-of-the-observerstealer-advertised-as-malware-as-a-service/

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

March 21, 2024 • 4:00 AM

More at www.hivepro.com