Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

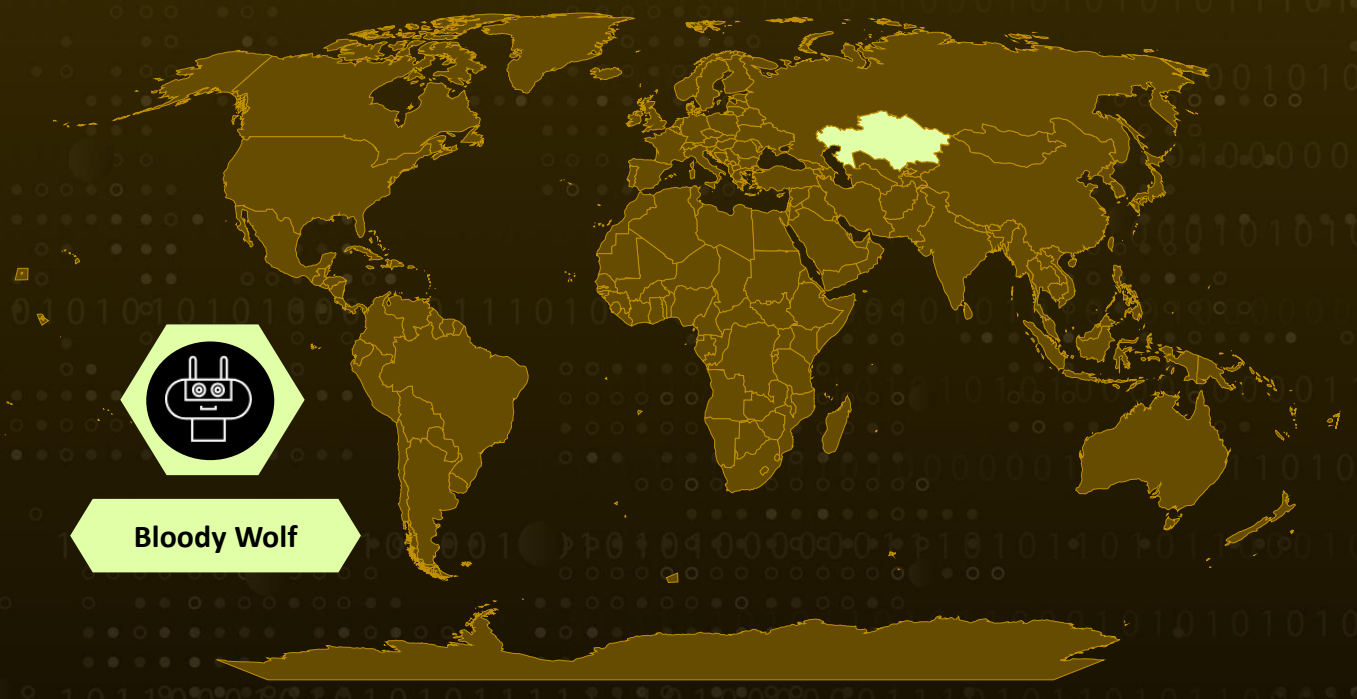
Bloody Wolf Targets Kazakhstan with STRRAT Malware

Date of Publication	Admiralty Code	TA Number
August 6, 2024	A1	TA2024298

Summary

Attack Began: 2023
Targeted Countries: Kazakhstan
Malware: STRRAT
Affected Platform: Windows
Threat Actor: Bloody Wolf
Attack: The Bloody Wolf threat group has been targeting organizations in Kazakhstan since late 2023 using STRRAT malware, which is available for purchase on underground forums. They employ sophisticated phishing tactics, impersonating government agencies to deliver malicious JAR files. Once installed, STRRAT exfiltrates sensitive data and allows remote control of compromised systems. The use of legitimate web services like Pastebin helps the attackers evade detection.

Attack Regions



Attack Details

#1 Bloody Wolf, a threat group, has been targeting organizations in Kazakhstan with a commodity malware called STRRAT (also known as Strigoi Master). The malware, which can be purchased for as little as $80 on underground forums, allows the attackers to take control of corporate computers and steal sensitive data.

#2 The cyber attacks employ sophisticated phishing tactics, impersonating the Ministry of Finance of the Republic of Kazakhstan and other government agencies. The phishing emails contain PDF attachments that appear to be non-compliance notices, but actually include links to a malicious Java archive (JAR) file and an installation guide for the Java interpreter necessary for the malware to function.

#3 The STRRAT malware, hosted on a website that mimics the government's website ("egov-kz[.]online"), sets up persistence on the Windows host by modifying the Registry and running the JAR file every 30 minutes. It also copies the JAR file to the Windows startup folder to ensure automatic execution after a system reboot.

#4 Once installed, the malware establishes connections with a Pastebin server to exfiltrate sensitive information from the compromised machine, including details about the operating system version, antivirus software installed, and account data from various browsers and email clients. It can also receive additional commands from the server to download and execute more payloads, log keystrokes, run commands using cmd.exe or PowerShell, restart or shut down the system, install a proxy, and remove itself.

#5 The use of less common file types like JAR enables the attackers to bypass defenses, while employing legitimate web services such as Pastebin to communicate with the compromised system makes it possible to evade network security solutions.

Recommendations

Enhance Email Security: Implement advanced email filtering solutions to detect and block phishing emails. Use email authentication protocols like SPF, DKIM, and DMARC to reduce email spoofing. Educate employees about the risks of phishing and train them to recognize suspicious email**s.**

Deploy Robust Endpoint Protection: Install and regularly update antivirus and anti-malware software on all endpoints. Use endpoint detection and response (EDR) solutions to monitor and respond to suspicious activities in real time.

Strengthen Network Security: Implement network segmentation to limit the spread of malware within the organization. Use firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS) to detect and block malicious traffic. Monitor network traffic for unusual activities and connections to known malicious domains.

Monitoring and Detection: Deploy advanced threat detection and monitoring tools capable of identifying and mitigating malware attacks in real-time. This includes behavior-based analytics, intrusion detection systems, and endpoint protection solutions.

Regular Software Updates: Keep all software, including operating systems and applications, updated with the latest patches to close vulnerabilities that malware can exploit.

Potential MITRE ATT&CK TTPs

TA0005 Defense Evasion	TA0040 Impact	TA0001 Initial Access	TA0002 Execution
TA0007 Discovery	TA0006 Credential Access	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	T1486 Data Encrypted for Impact	T1566 Phishing

T1566.001 Spearphishing Attachment	T1204 User Execution	T1566.002 Spearphishing Link	T1059.003 Windows Command Shell
T1059.005 Visual Basic	T1204.002 Malicious File	T1083 File and Directory Discovery	T1059.007 JavaScript
T1053.005 Scheduled Task	T1053 Scheduled Task/Job	T1059 Command and Scripting Interpreter	T1136 Create Account
T1136.001 Local Account	T1547.001 Registry Run Keys / Startup Folder	T1055 Process Injection	T1036 Masquerading
T1547 Boot or Logon Autostart Execution	T1134 Access Token Manipulation	T1134.002 Create Process with Token	T1070.004 File Deletion
T1070 Indicator Removal	T1057 Process Discovery	T1112 Modify Registry	T1564.003 Hidden Window
T1082 System Information Discovery	T1564 Hide Artifacts	T1056.001 Keylogging	T1056 Input Capture
T1185 Browser Session Hijacking	T1113 Screen Capture	T1518 Software Discovery	T1555 Credentials from Password Stores
T1090.001 Internal Proxy	T1090 Proxy	T1518.001 Security Software Discovery	T1555.003 Credentials from Web Browsers
T1102 Web Service	T1105 Ingress Tool Transfer	T1529 System Shutdown/Reboot	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	e35370cb7c8691b5fdd9f57f3f462807b40b067e305ce30eabc16e0642eca06b, 00172976ee3057dd6555734af28759add7daea55047eb6f627e5491701c3ec83, cb55cf3e486f3cbe3756b9b3abf1673099384a64127c99d9065aa26433281167, a6fb286732466178768b494103e59a9e143d77d49445a876ebd3a40904e2f0b0, 25c622e702b68fd561db1aec392ac01742e757724dd5276b348c11b6c5e23e59, 14ec3d03602467f8ad2e26eef7ce950f67826d23fedb16f30d5cf9c99dfeb058, ee113a592431014f44547b144934a470a1f7ab4abec70ba1052a4feb3d15d5c6
IPv4	91[.]92[.]240[.]188, 185[.]196[.]10[.]116
URLs	hxxps[:]//pastebin[.]com/raw/dFKy3ZDm[:]13570, hxxps[:]//pastebin[.]com/raw/dLzt4tRB[:]13569, hxxps[:]//pastebin[.]com/raw/dLzt4tRB[:]10101, hxxps[:]//pastebin[.]com/raw/YZLySxsv[:]20202, hxxps[:]//pastebin[.]com/raw/8umPhg86[:]13772, hxxps[:]//pastebin[.]com/raw/67b8GSUQ[:]13671, hxxps[:]//pastebin[.]com/raw/8umPhg86[:]13771, hxxps[:]//pastebin[.]com/raw/67b8GSUQ[:]13672, hxxps[:]//pastebin[.]com/raw/dLzt4tRB[:]13880, hxxps[:]//pastebin[.]com/raw/YZLySxsv[:]13881

References

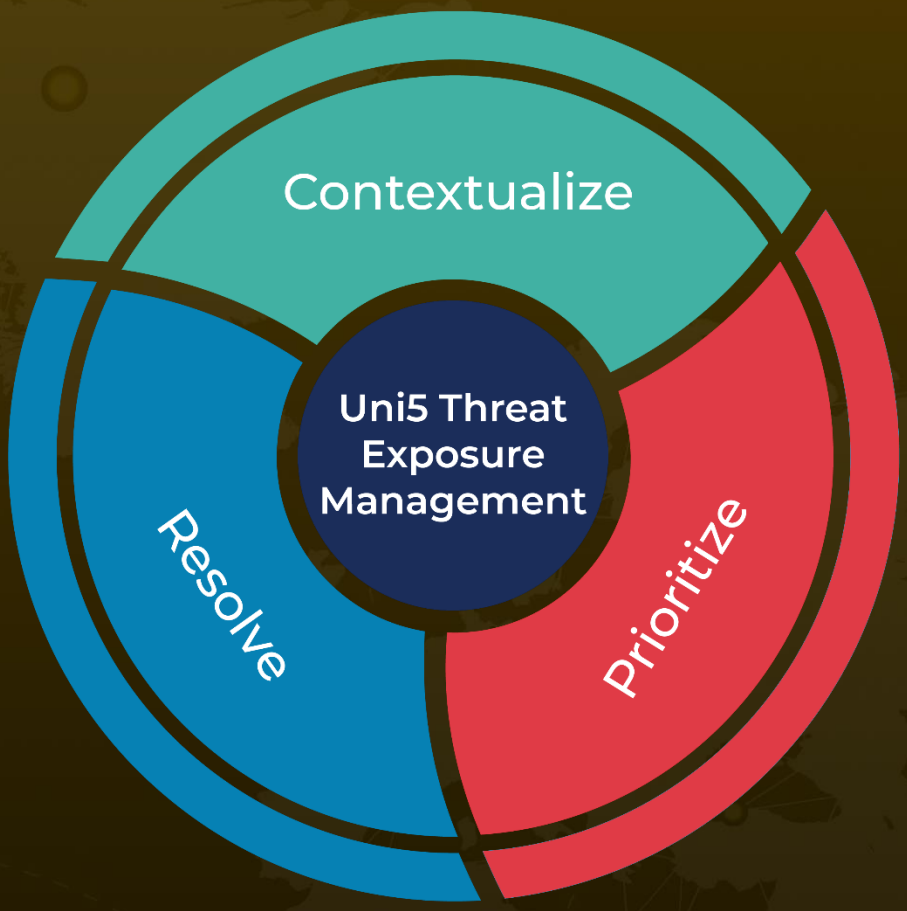
https://bi.zone/eng/expertise/blog/bloody-wolf-primenyaet-kommercheskoe-vpo-strrat-protiv-organizatsiy-v-kazakhstane/

https://www.hivepro.com/strrat-a-java-powered-versatile-remote-access-trojan/

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

August 6, 2024 • 6:00 AM

More at www.hivepro.com