Hive Pro®

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

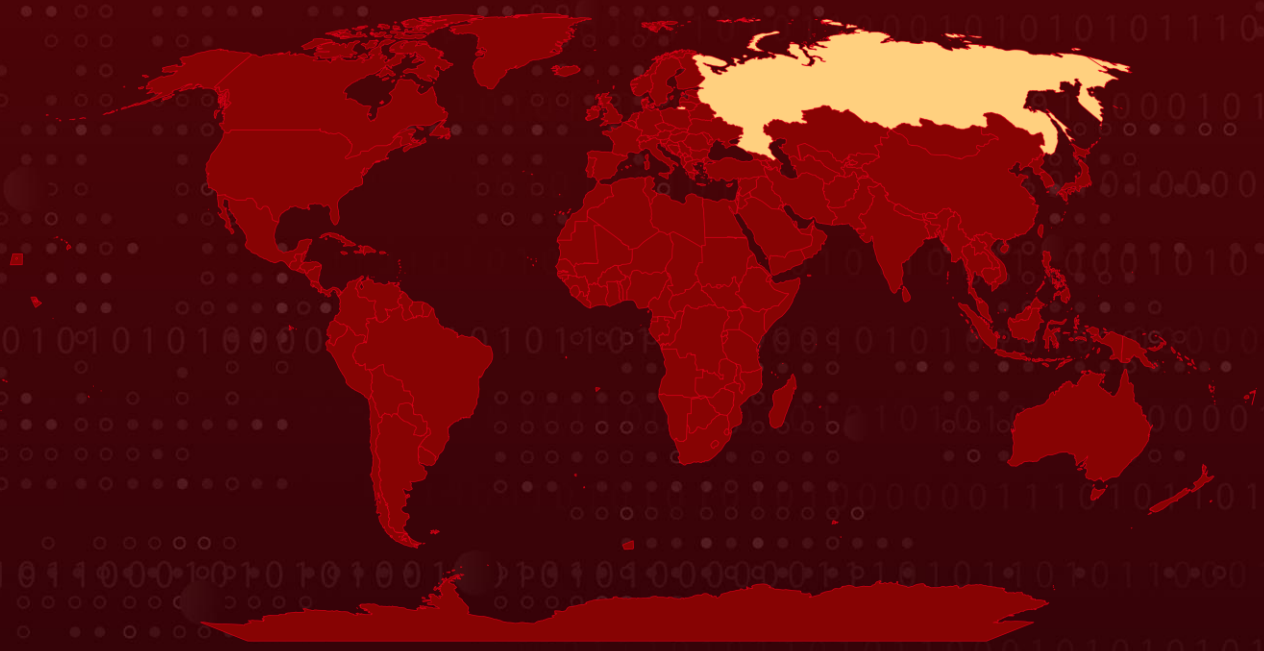
Dissemination of the Konni Campaign Through Malicious Documents

Date of Publication	Admiralty Code	TA Number
November 24, 2023	A1	TA2023474

Summary

Attack Began: September 2023
Attack Region: Russia
Affected Platform: Microsoft Windows
Attack: The Konni campaign has resurfaced in a new phishing attack employing a Russian-language Microsoft Word document to distribute malware. The malicious software aims to harvest sensitive information from compromised Windows hosts.

Attack Regions



Attack Details

#1 In a recent Konni Campaign, a Russian-language Microsoft Word document was used to deliver malware designed for harvesting sensitive information from compromised Windows hosts. This campaign involves a remote access trojan (RAT) that allows remote attackers to assume control of the infected systems, facilitating the extraction of information and execution of commands as part of its malicious activities.

#2 Konni's primary objectives encompass data espionage activities. The most recent observed attack involves the use of a macro-laced Word document. Upon enabling the macros, the document displays an article in Russian, purportedly discussing "Western Assessments of the Progress of the Special Military Operation.“

#3 The VBA script extracts information from "OLEFormat.IconLabel" and saves it in a temporary folder. It then runs the "check.bat" script with the "vbHide" parameter to execute silently. The script verifies the presence of remote connection sessions, Windows 10 operating systems, and 64-bit architectures. If these conditions are met, it triggers the "netpp.bat" script.

#4 The "check.bat" batch file employs "wpns.dll" to bypass User Account Control (UAC) by launching "wusa.exe," a legitimate Windows utility. This process operates with elevated privileges, duplicates its access token, and executes a command via “CreateProcessWithLogonW”. It then executes a "netpp.bat" script, inheriting the elevated privileges and copying the final payload, creating service and registry entries for persistence.

#5 The DLL files embedded within the Word document are compressed using UPX. The utilization of these batch scripts and DLL files reveals an advanced toolset employed by a highly skilled threat actor within a Word document. Users are advised to exercise caution when opening any suspicious documents, as this malware is continuously evolving.

Recommendations

Educate Users: Train users to be cautious when opening email attachments, especially those from unknown or unexpected sources. Warn them about the potential dangers of enabling macros in documents to prevent successful phishing attempts.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Network Segmentation: Implement proper network segmentation to limit the lateral movement of malware within the network. By dividing the network into smaller, isolated segments, organizations can contain the spread of malware and prevent it from accessing critical systems and sensitive data.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation
TA0005 Defense Evasion	TA0007 Discovery	TA0009 Collection	TA0010 Exfiltration
T1574 Hijack Execution Flow	T1027 Obfuscated Files or Information	T1134 Access Token Manipulation	T1569 System Services
T1543 Create or Modify System Process	T1543.003 Windows Service	T1082 System Information Discovery	T1059 Command and Scripting Interpreter
T1059.005 Visual Basic	T1204 User Execution	T1204.002 Malicious File	T1560 Archive Collected Data
T1548 Abuse Elevation Control Mechanism	T1566 Phishing	T1140 Deobfuscate/Decode Files or Information	T1547 Boot or Logon Autostart Execution

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	kmdqj1[.]c1[.]biz, ouvxu2[.]c1[.]biz, 9b31n8[.]c1[.]biz, 3pl0y5[.]c1[.]biz, dpgbep[.]c1[.]biz, 7qnbae[.]c1[.]biz, glws5m[.]c1[.]biz, ewqqa4[.]c1[.]biz, 3897lb[.]c1[.]biz, 558ga9[.]c1[.]biz, b91stf[.]c1[.]biz, bg5pl1[.]c1[.]biz, caoy9n[.]c1[.]biz, rziju6[.]c1[.]biz, pm90p1[.]c1[.]biz, pxyunf[.]c1[.]biz, m2jymd[.]c1[.]biz, aocsff[.]c1[.]biz, 6e2nbc[.]c1[.]biz, vqt9i1[.]c1[.]biz
SHA256	ac9b814b98a962bc77b2ab862d9c3b1ba5f7e86b80797259b4fcb40bfb389081, f07e55ce20e944706232013241d23282e652de2c9514904dede14d4a711a5d1d, 085cdb09aba0024c0cadbefe428817829bbe4ab0f68598572ebccc2f6f25e78f, 793b8e72fded73ae6839e678b03bd5c99959f47a1ad632095ba60fb89f66fa91, 83e66d912ca592bc2accfd9c275647f287b6dc72a859054a348e616537999b64, 656dd6e67a51aebc6c69dc35eaba2e1502f225ae6fd9d0a5ff70879982427844, cfbc7e6a89e4a23a72c7bcd9019197721f18506d9ab842011e0ab9d9eb24c2cc

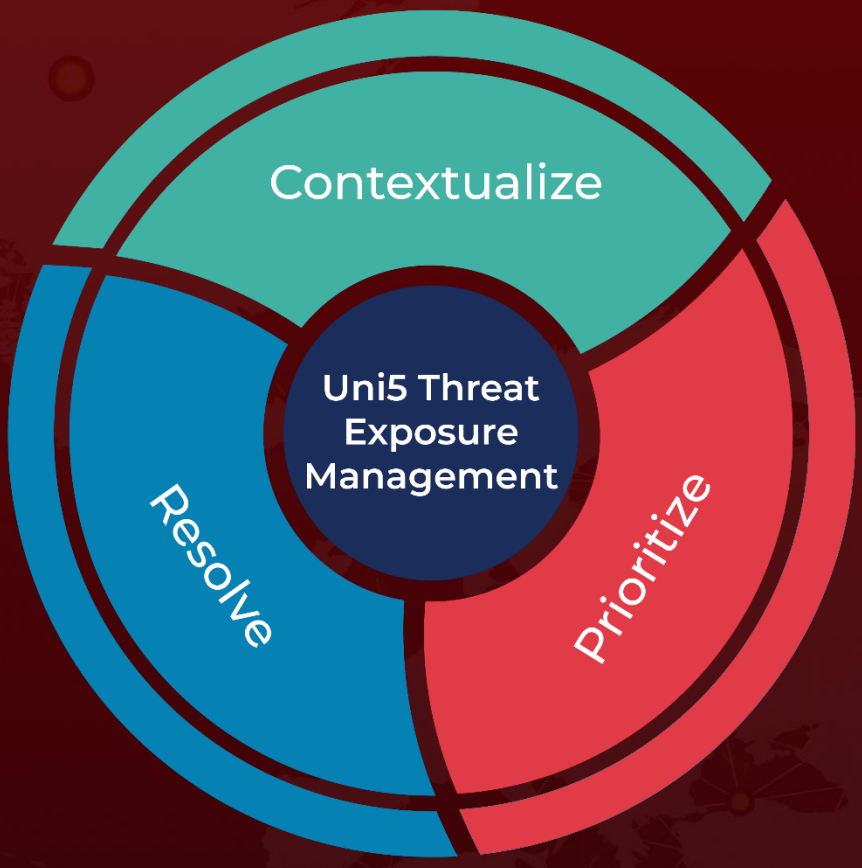
References

https://www.fortinet.com/blog/threat-research/konni-campaign-distributed-via-malicious-document

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

November 24, 2023 . 4:45 AM

More at www.hivepro.com