Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

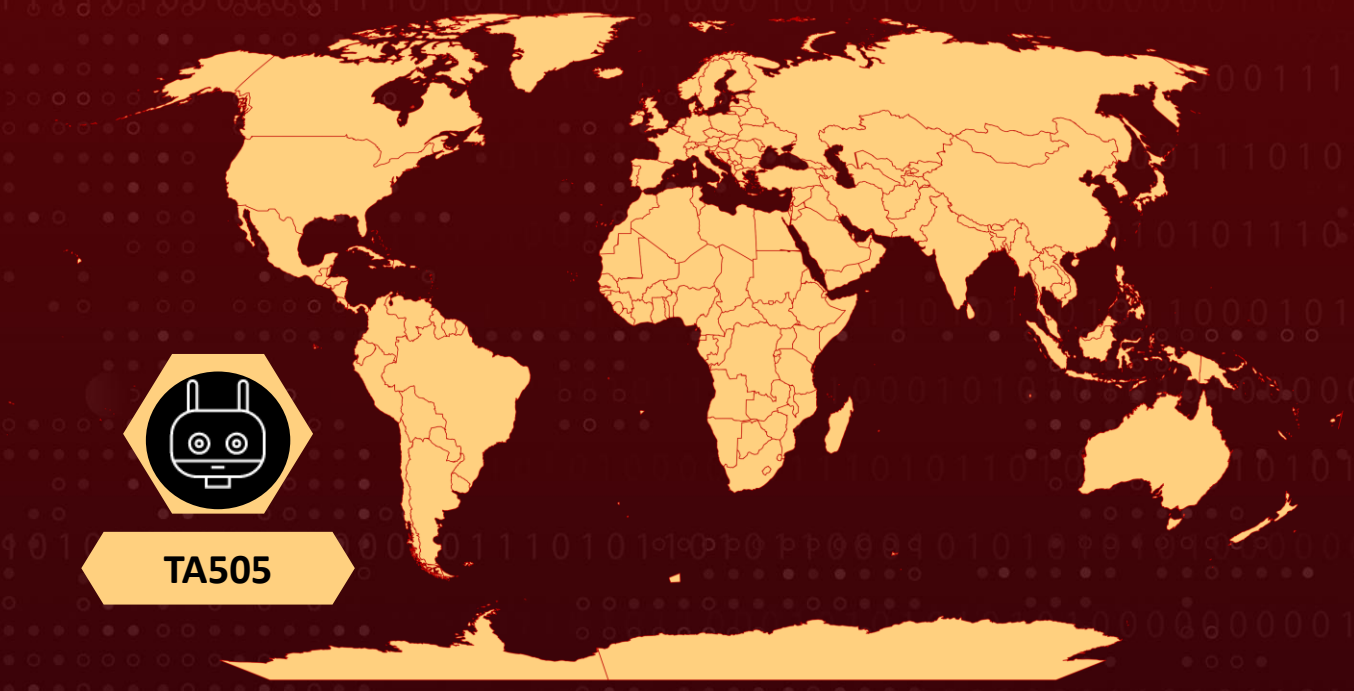
New LOBSHOT Malware Being Distributed Through Google Ads

Date of Publication	Admiralty Code	TA Number
May 04, 2023	A1	TA2023209

Summary

First Appearance: July, 2022
Malware: LOBSHOT
Targeted Countries: Worldwide
Threat Actor: TA505
Affected Platforms: Windows
Attack: LOBSHOT is a new malware that is being distributed through Google Ads. It is a remote access trojan that can allow threat actors to take control of an infected Windows device's hidden desktop, execute commands, steal data, and deploy further malware payloads.

Attack Regions



Attack Details

#1 A new malware, known as LOBSHOT, is being distributed through Google Ads. The ads claim to promote the legitimate AnyDesk remote management software but lead to a fake AnyDesk site at amydeecke[.]website, which pushes a malicious MSI file. The cybercrime group TA505 has been using LOBSHOT since 2022.

#2 LOBSHOT's primary function is its Hidden Virtual Network Computing (hVNC) feature, which allows the attacker to gain direct and undetected access to the infected device. The malware uses simple encryption methods and custom structures to hide its strings and collect data from the infected machine before sending any network requests.

#3 Upon execution, LOBSHOT copies itself to C:\ProgramData, launches a new process using explorer.exe, terminates the original process, and deletes the original file. The malware is a remote access trojan that installs an hVNC module, allowing threat actors to take control of the infected Windows device's hidden desktop and execute commands, steal data, and deploy further malware payloads.

#4 The threat actors can operate the device using their mouse and keyboard as if they were in front of it. This type of access could lead to ransomware attacks, data extortion, and other attacks, and it is likely used for initial access to corporate networks and to spread laterally to other devices.

Recommendations

As LOBSHOT is being distributed through fake websites and Google Ads, it is crucial to only download software from trusted sources. Users should be cautious when clicking on ads, especially those that promote software downloads.

LOBSHOT could potentially exploit vulnerabilities in outdated software to gain access to a system. Therefore, it is essential to keep all software and operating systems up-to-date with the latest security patches and updates.

Implementing a multi-layered security approach can help detect and prevent malware like LOBSHOT. This could include using anti-virus software, firewalls, intrusion detection and prevention systems, and implementing strong access controls and authentication mechanisms.

Potential MITRE ATT&CK TTPs

TA0003 Persistence	TA0002 Execution	TA0007 Discovery	TA0004 Privilege Escalation
TA0011 Command and Control	TA0009 Collection	TA0005 Defense Evasion	TA0040 Impact
TA0001 Initial Access	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1027 Obfuscated Files or Information
T1027.007 Dynamic API Resolution	T1140 Deobfuscate/Decode Files or Information	T1568 Dynamic Resolution	T1005 Data from Local System
T1083 File and Directory Discovery	T1033 System Owner/User Discovery	T1021 Remote Services	T1204 User Execution
T1204.002 Malicious File	T1021.005 VNC	T1041 Exfiltration Over C2 Channel	T1218 System Binary Proxy Execution
T1176 Browser Extensions	T1641 Data Manipulation	T1115 Clipboard Data	T1321 Data Encoding
T1189 Drive-by Compromise			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPV4	95.217.125[.]200
SHA256	e4ea88887753a936eaf3361dcc00380b88b0c210dcbde24f8f7ce27991856bf6

References

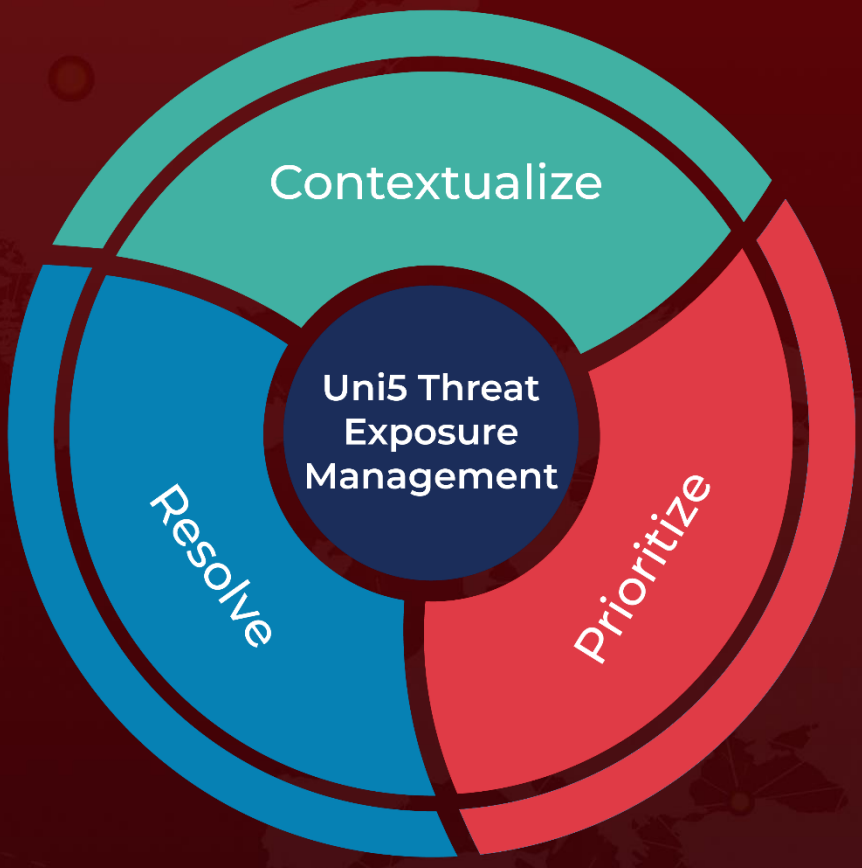
https://www.elastic.co/security-labs/elastic-security-labs-discovers-lobshot-malware

https://www.bleepingcomputer.com/news/security/new-lobshot-malware-gives-hackers-hidden-vnc-access-to-windows-devices/

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

May 04, 2023 • 6:30 AM

More at www.hivepro.com