Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

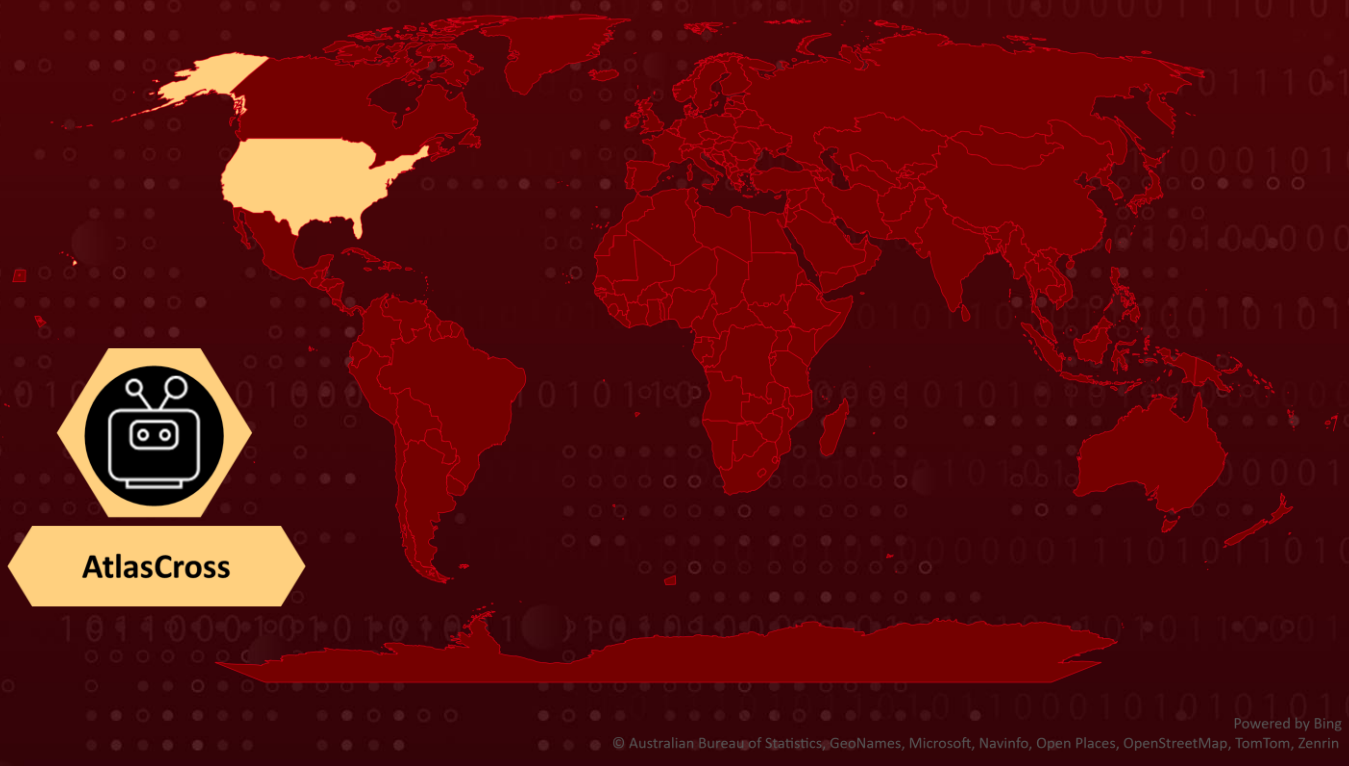
AtlasCross Exploits Organizations with DangerAds and AtlasAgent Trojans

Date of Publication	Admiralty Code	TA Number
September 28, 2023	A1	TA2023391

Summary

Attack Began: September 2023
Attack Region: United States
Affected Industries: Healthcare
Actor Name: AtlasCross
Malware: DangerAds, AtlasAgent
Attack: A new threat actor by the name of AtlasCross has been identified employing phishing tactics that use Red Cross-themed lures as part of their attack strategy. These phishing campaigns are being used to distribute two previously unidentified trojans known as DangerAds and AtlasAgent.

Attack Regions



Attack Details

#1 A new Advanced Persistent Threat (APT) actor, referred to as AtlasCross, has emerged with a primary focus on conducting targeted attacks against specific hosts within a network domain. This threat actor is employing Red Cross-themed phishing lures as part of their attack tactics to deliver two previously unidentified trojans, known as DangerAds and AtlasAgent. The phishing attack activity that has been captured is a crucial element of the attacker's broader strategy aimed at specific targets.

#2 The attack chains commence with a Microsoft document that has been injected with a malicious macro. This document typically disguises itself as information related to a blood donation drive organized by the American Red Cross. When a victim opens this document and activates the embedded malicious macro, leading to the establishment of a persistent presence, and the exfiltration of system metadata to a remote server hosted at "data.vectorse[.]com." Remarkably, this server is a sub-domain of a legitimate website associated with a U.S.-based structural and engineering company.

#3 This attack process can be segmented into three distinct phases: the decoy document phase, the loader phase, and the Trojan horse phase. In the initial phase of the attack flow, which is the decoy document phase, malicious macrocode embedded within the decoy document comes into play. The primary functions of this malicious macro involve deploying a payload, configuring scheduled tasks, and uploading essential information about the victim's host.

#4 The program known as KB4495667.pkg, introduced by the malicious macrocode, plays a central role in the second phase of this attack sequence. In parallel, the same malicious macro extracts another file, labeled DangerAds, which functions as a loader. This loader's purpose is to execute shellcode that initiates the deployment of AtlasAgent, a versatile C++ malware with a range of capabilities. AtlasAgent is adept at gathering system information, conducting shellcode operations, executing commands for establishing a reverse shell, and injecting code into a designated process's specific thread.

#5 The DangerAds will eventually load either an x86 or x64 version of a DLL program into memory, with AtlasAgent serving as the final payload in this attack sequence for the final phase.

Recommendations

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 malware from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Email Security: Enhance email security measures and educate users on recognizing social engineering tactics to mitigate the risk of falling prey to phishing attacks leveraging deceptive zip file attachments.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	**TA0003** Persistence	**TA0005** Defense Evasion	**TA0011** Command and Control
TA0007 Discovery	**T1053** Scheduled Task/Job	**T1055** Process Injection	**T1620** Reflective Code Loading
T1001 Data Obfuscation	**T1027** Obfuscated Files or Information	**T1027.005** Indicator Removal from Tools	**T1134** Access Token Manipulation
T1218 System Binary Proxy Execution	**T1218.011** Rundll32	**T1497** Virtualization/Sandbox Evasion	**T1562** Impair Defenses
T1562.001 Disable or Modify Tools	**T1016** System Network Configuration Discovery	**T1583** Acquire Infrastructure	**T1518** Software Discovery
T1105 Ingress Tool Transfer	**T1573** Encrypted Channel	**T1082** System Information Discovery	

Indicators of Compromise (IOCs)

TYPE	VALUE
Domains	data.vectorse[.]com, activequest.goautodial[.]com, ops-ca.mioying[.]com, app.basekwt[.]com, secure.poliigon[.]com, engage.adaptqe[.]com, chat.thedresscodeapp[.]com, superapi-staging.mlmprotec[.]com, search.allaccountingcareers[.]com, order.staging.photobookworldwide[.]com, crm.cardabel[.]com, public.pusulait[.]com
Filepath	%USERPROFILE%\Documents\Code\atlasagent\x64\Release\AtlasDLL.pdb
MD5	7195d7e4926a0a85fbe81e40ab7c0ca4, F8bafe2ce6f11a32109abbab1c42e2cf, ca48431273dfcd2bd025e55f2de30635, ba85467ceff628be8b4f0e2da2a5990c

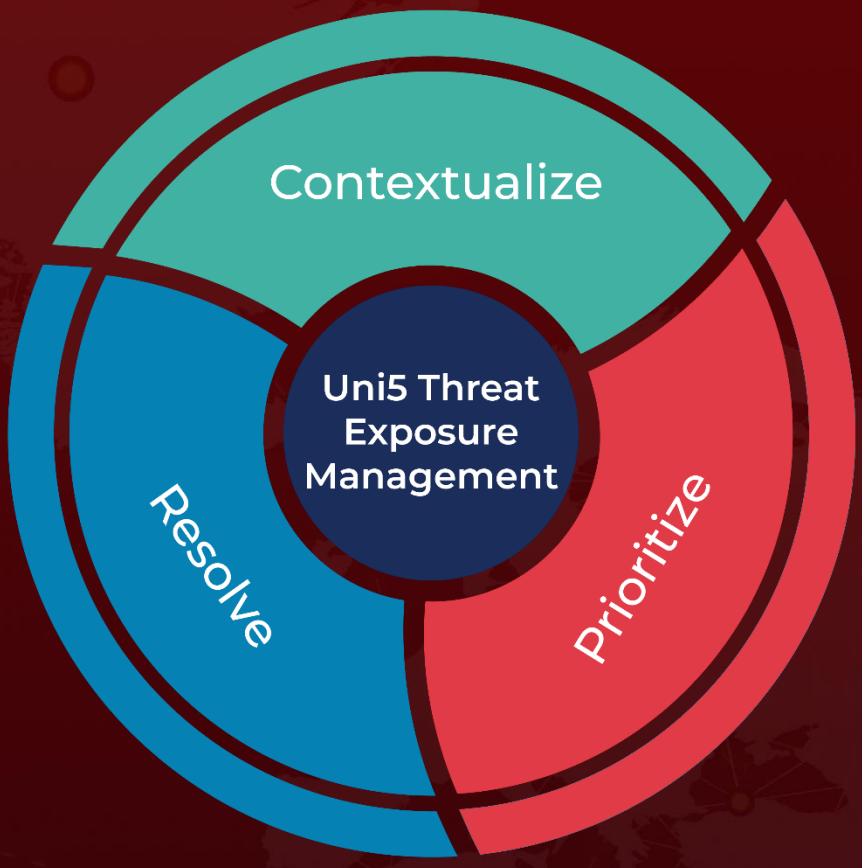
References

https://nsfocusglobal.com/warning-newly-discovered-apt-attacker-atlascross-exploits-red-cross-blood-drive-phishing-for-cyberattack/

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

September 28, 2023 . 5:45 AM

More at www.hivepro.com