Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

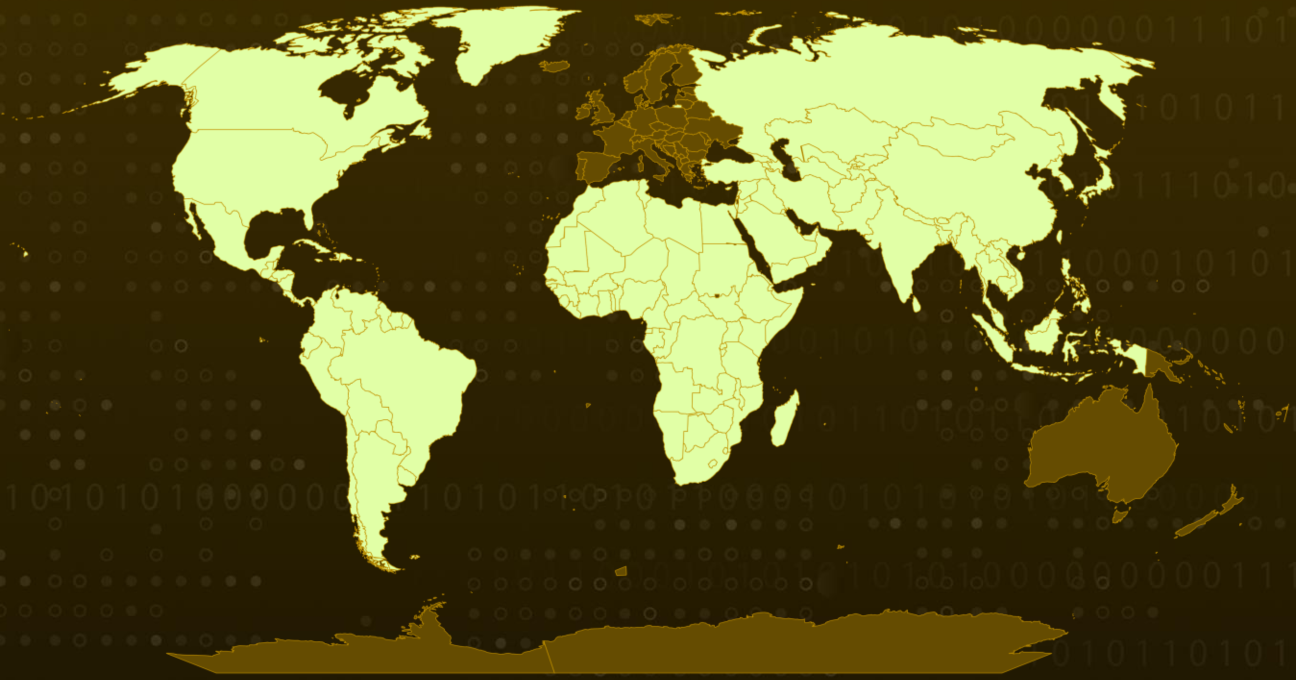
Revealing DarkGate's Incursion Across Continents

Date of Publication	Admiralty Code	TA Number
October 13, 2023	A1	TA2023415

Summary

First Seen: 2017
Malware: DarkGate (aka Meh)
Attack Region: Americas region, Asia, the Middle East, and Africa
Attack: A potential threat actor has been using compromised Skype and Microsoft Teams accounts to distribute DarkGate, a problematic loader campaign primarily targeting the Americas region.

Attack Regions



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

Attack Details

#1 A potential threat actor has been utilizing compromised Skype and Microsoft Teams accounts to disseminate DarkGate, a problematic loader associated with various malicious activities observed from July to September. This loader, categorized as a commodity loader, was initially documented in late 2017 and has gained traction since its appearance on the Russian language forum eCrime in May 2023.

#2 The recent DarkGate campaign was first detected in the Americas region and later identified in Asia, the Middle East, and Africa. The primary goals of these activities involve information theft, keylogging, and the deployment of cryptocurrency miners. While the method used to compromise the originating Skype and Microsoft Teams accounts is still unclear.

#3 There are hypotheses suggesting it may have stemmed from leaked credentials available on underground forums or a prior compromise of the parent organization. The threat actor exploited a trusted relationship between the two organizations, tricking recipients into executing the attached VBA script.

#4 DarkGate employs a Windows-specific automation and scripting tool known as AutoIt to deliver and execute its malicious functionalities. To ensure persistence, the malware drops a randomly named LNK file into the Windows User Startup folder, enabling automatic execution at every system startup.

#5 Post-installation, the detected files are variants of either DarkGate or Remcos, potentially indicating an effort to strengthen the attackers' foothold in the infected system. The motivations of these adversaries may vary, emphasizing the importance for organizations to remain vigilant against threat actors employing DarkGate to infect systems with diverse forms of malware.

Recommendations

Enforce Instant Messaging Security Policies: Develop and enforce stringent security policies for instant messaging applications, specifically Skype and Microsoft Teams. Implement rules that restrict communication with external domains, minimizing the risk of unauthorized access and data exfiltration.

Role-Based Access Control (RBAC): Enforce RBAC to ensure that users have the minimum necessary privileges to perform their roles. Limiting access rights reduces the impact of compromised credentials.

Behavioral Anomaly Detection: Deploy advanced behavioral anomaly detection systems that can identify deviations from normal user and system behavior, flagging activities such as frequent and unusual execution of reconnaissance commands.

Zero Trust Model: Adopt a Zero Trust security model, which requires verification from anyone trying to access resources on a network, regardless of location, to minimize the attack surface.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0042** Resource Development	**TA0001** Initial Access	**TA0002** Execution
TA0003 Persistence	**TA0004** Privilege Escalation	**TA0005** Defense Evasion	**TA0006** Credential Access
TA0011 Command and Control	**T1589** Gather Victim Identity Information	**T1586** Compromise Accounts	**T1608** Stage Capabilities
T1133 External Remote Services	**T1059** Command and Scripting Interpreter	**T1569** System Services	**T1547** Boot or Logon Autostart Execution

T1543 Create or Modify System Process	T1055 Process Injection	T1211 Exploitation for Defense Evasion	T1056.001 Keylogging
T1057 Process Discovery	T1570 Lateral Tool Transfer	T1105 Ingress Tool Transfer	T1056 Input Capture
T1059.005 Visual Basic	T1036 Masquerading		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	4ed69ed4282f5641b5425a9fca4374a17aecb160, 549cb39cea44cf8ca7d781cd4588e9258bdff2a1, e108fe723265d885a51e9b6125d151b32e23a949, a85664a8b304904e7cd1c407d012d3575eeb2354, 924b60bd15df000296fc2b9f179df9635ae5bfed, cec7429d24c306ba5ae8344be831770dfe680da4, d9a2ae9f5cffba0d969ef8edbbf59dc50586df00, 381bf78b64fcdf4e21e6e927edd924ba01fdf03d, 4c24d0fc57633d2befaac9ac5706cbc163df747c, 9253eed158079b5323d6f030e925d35d47756c10, 0e7b5d0797c369dd1185612f92991f41b1a7bfa2, 7d3f4c9a43827bff3303bf73ddbb694f02cc7ecc, e47086abe1346c40f58d58343367fd72165ddecd, 42fe509513cd0c026559d3daf491a99914fcc45b, 93cb5837a145d688982b95fab297ebdb9f3016bc, f7b9569a536514e70b6640d74268121162326065, d40c7afee0dd9877bbe894bc9f357b50e002b7e2, 1f550b3b5f739b74cc5fd1659d63b4a22d53a3fc, 3229a36f803346c513dbb5d6fe911d4cb2f4dab1, 6585e15d53501c7f713010a0621b99e9097064ff, 001e4eacb4dd47fa9f49ff20b5a83d3542ad6ba2, ad1667eaf03d3989e5044faa83f6bb95a023e269, a3516b2bb5c60b23b4b41f64e32d57b5b4c33574, e6347dfdaf3f1e26d55fc0ed3ebf09b8e8d60b3f, 3cbbdfc83c4ef05c0f5c37c99467958051f4a0e1, f3a740ea4e04d970c37d82617f05b0f209f72789, e6e4c7c2c2c8e370a0ec6ddb5d998c150dcb9f10, 45a89d03016695ad87304a0dfd04648e8dfeac8f

TYPE	VALUE
Domain	msteamseyeappstore[.]com, Drkgatevservicceoffice[.]net, reactervnamnat[.]com, coocooncookiedpo[.]com, wmnwserviceadsmark[.]com, onlysportsfitnessam[.]com, marketisportsstumi[.]win
IPv4:Port	5.188.87[.]58[:]2351
URL	hxxp://corialopolova.com/vHdLtiAzZYCsHszzP118[.]bin

References

https://www.trendmicro.com/en_us/research/23/j/darkgate-opens-organizations-for-attack-via-skype-teams.html

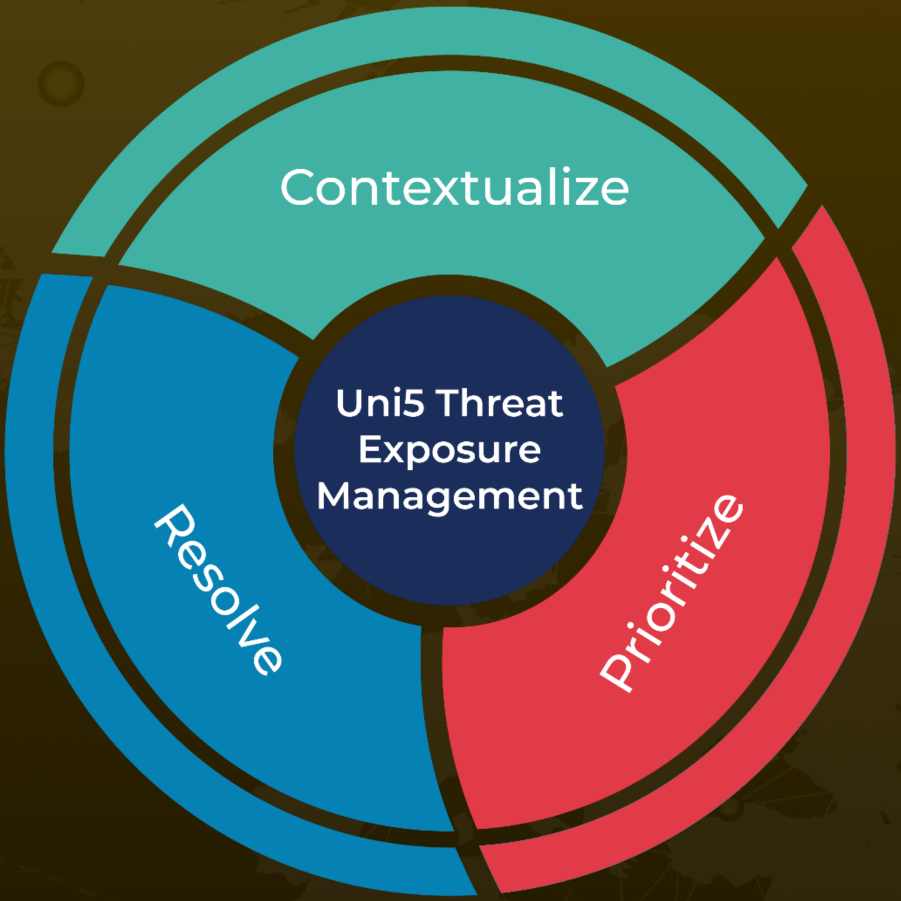
https://www.trendmicro.com/content/dam/trendmicro/global/en/research/23/j/darkgate-opens-organizations-for-attack-via-skype-teams/IOCs-DarkGate-Opens-Organizations-for-Attack-via-Skype-Teams.txt

https://github.com/prodaft/malware-ioc/blob/master/PTI-66/DarkGate.md

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

October 13, 2023 • 5:00 AM

More at www.hivepro.com