GENERAL DYNAMICS

May 2020

Lazarus Group Activity (GD-ISAC) Reporting

By

Joseph Taddeo
General Dynamics Information Sharing and Analysis Center
(GD ISAC)

GENERAL DYNAMICS

This report has been cleared for Public release, all victims have been redacted.

GENERAL DYNAMICS

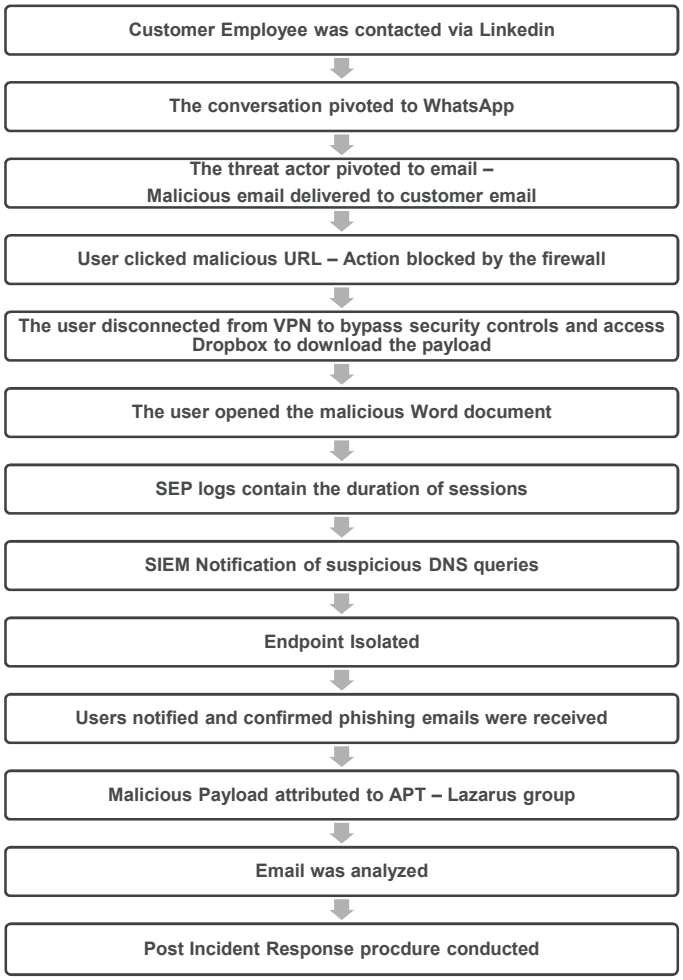
Executive Summary

The General Dynamics Information Sharing and Analysis Center (GD-ISAC) detected an attempted compromise of information technology systems potentially attributed to APT 38 – Lazarus Group. This attempted compromise was a sophisticated attack that moved across several threat vectors resulting in a malicious payload being executed but was blocked by security appliances supplied with IOCs from the GD-ISAC—utilizing automated delivery of IOCs to the customers SIEM and subsequently endpoint devices.

Threat Vectors

LinkedIn → WhatsApp → BU Email → User Endpoint

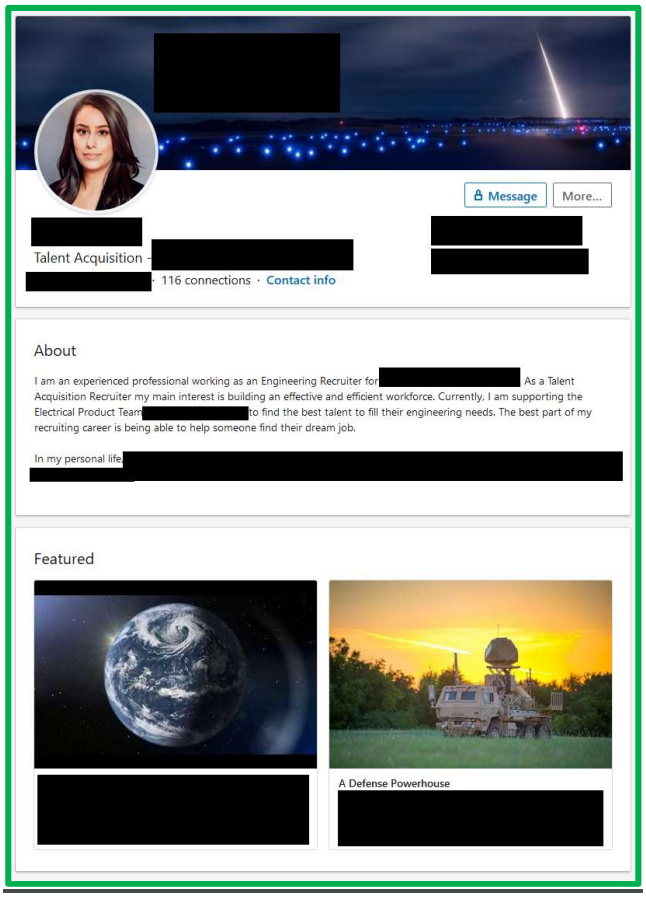
Order of Events



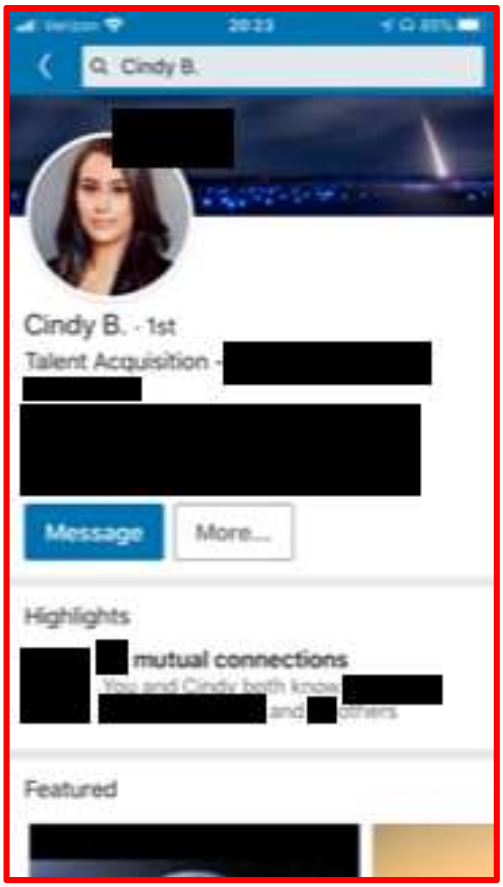
GENERAL DYNAMICS

LinkedIn Profile of Company Employee

Real Recruiter – This picture is a legitimate profile of a talent acquisition employee at Company B



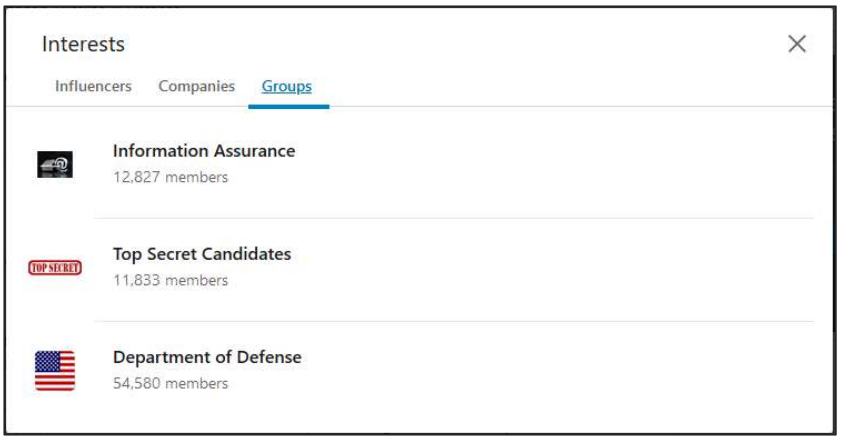
Fake Recruiter – This picture is the fake persona that initiated contact with customer employee



GENERAL DYNAMICS

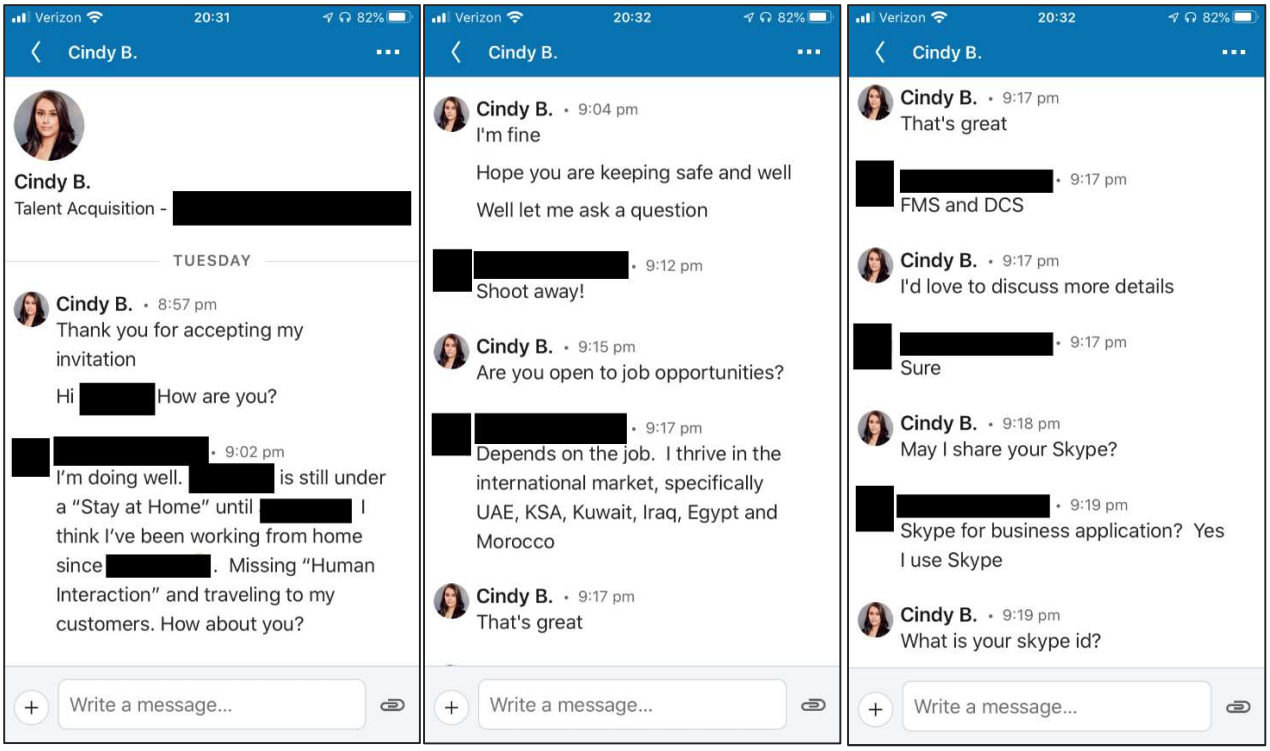
Recruiter's Interested Groups on LinkedIn

The interests of the recruiter's LinkedIn profile indicate that Top Secret, DoD, and Information assurance professionals could potentially be targeted. It is likely that these and similar groups containing defense industrial base and cleared professionals are hunting grounds for threat actors.



Threat Vector - LinkedIn messenger

The following screenshots are from a conversation between the threat actor spoofing the recruiter's profile and a Program Manager from a GD-ISAC customer.

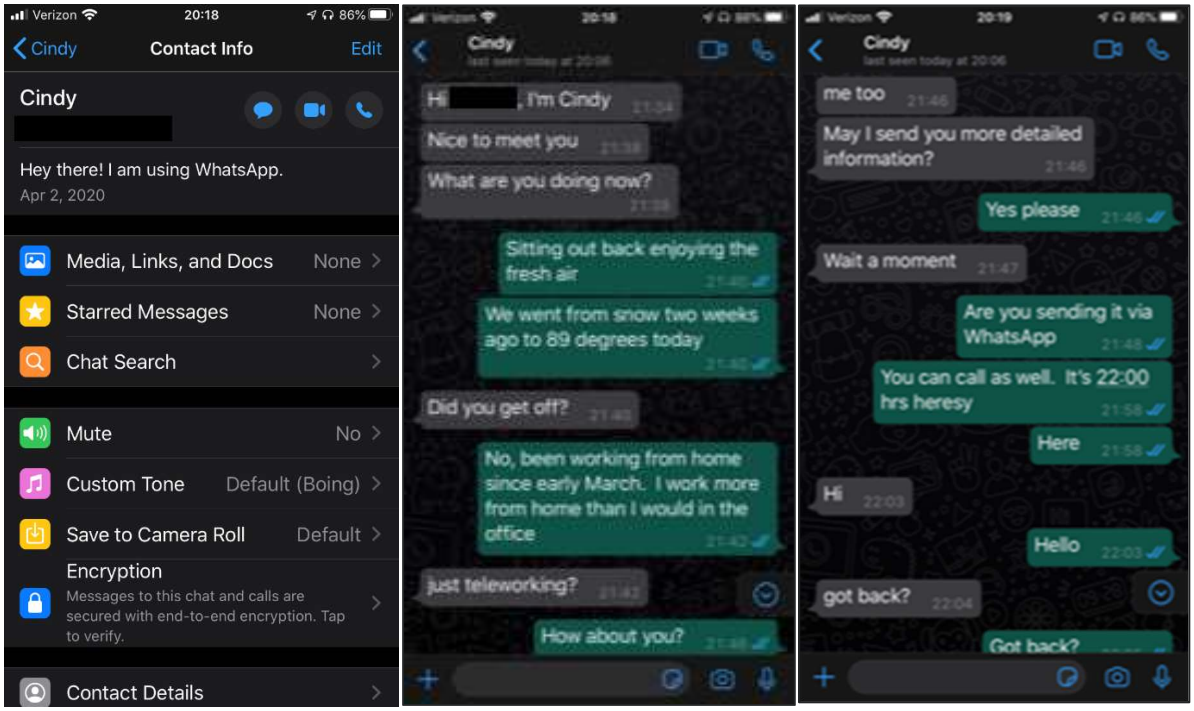


GENERAL DYNAMICS

Threat Vector - LinkedIn messenger – Continued

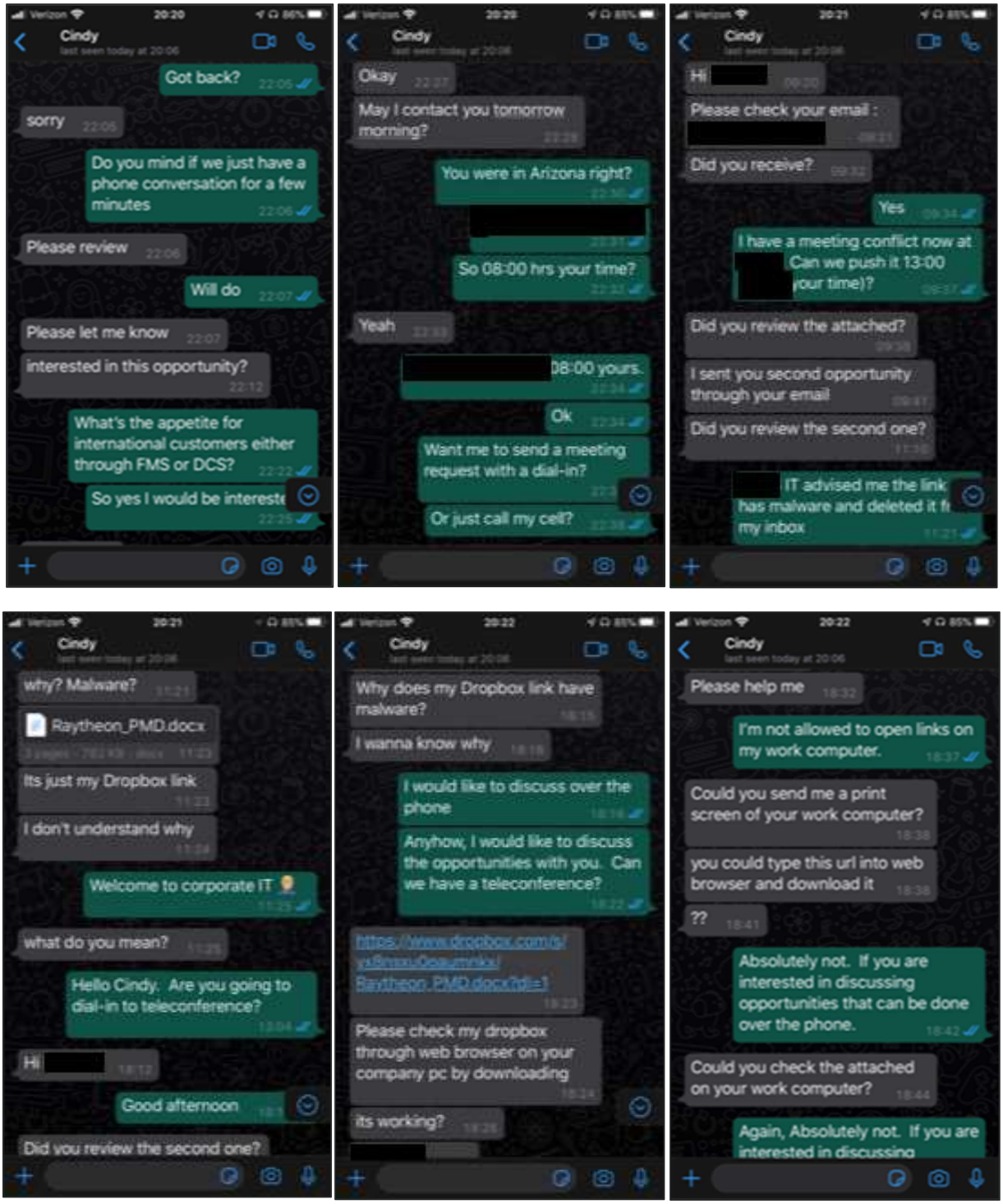
Threat Vector – WhatsApp

These screenshots are from the conversation once the parties moved to WhatsApp. The differences between the syntax in the first and second set of screenshots indicates the threat actor from LinkedIn and WhatsApp could be different people from the same threat actor group.



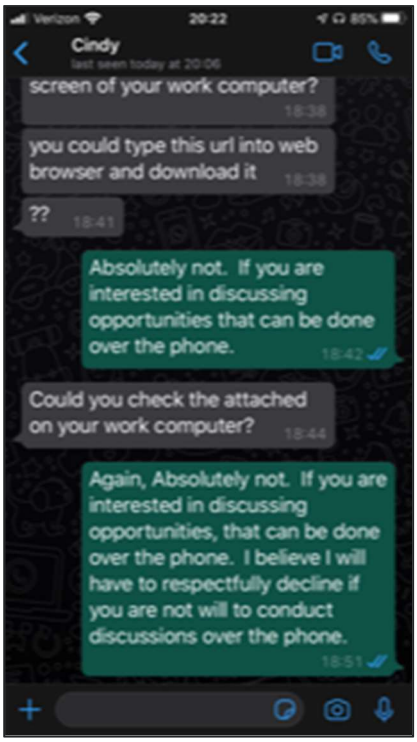
GENERAL DYNAMICS

Threat Vector – WhatsApp – Continued



GENERAL DYNAMICS

Threat Vector – WhatsApp – Continued



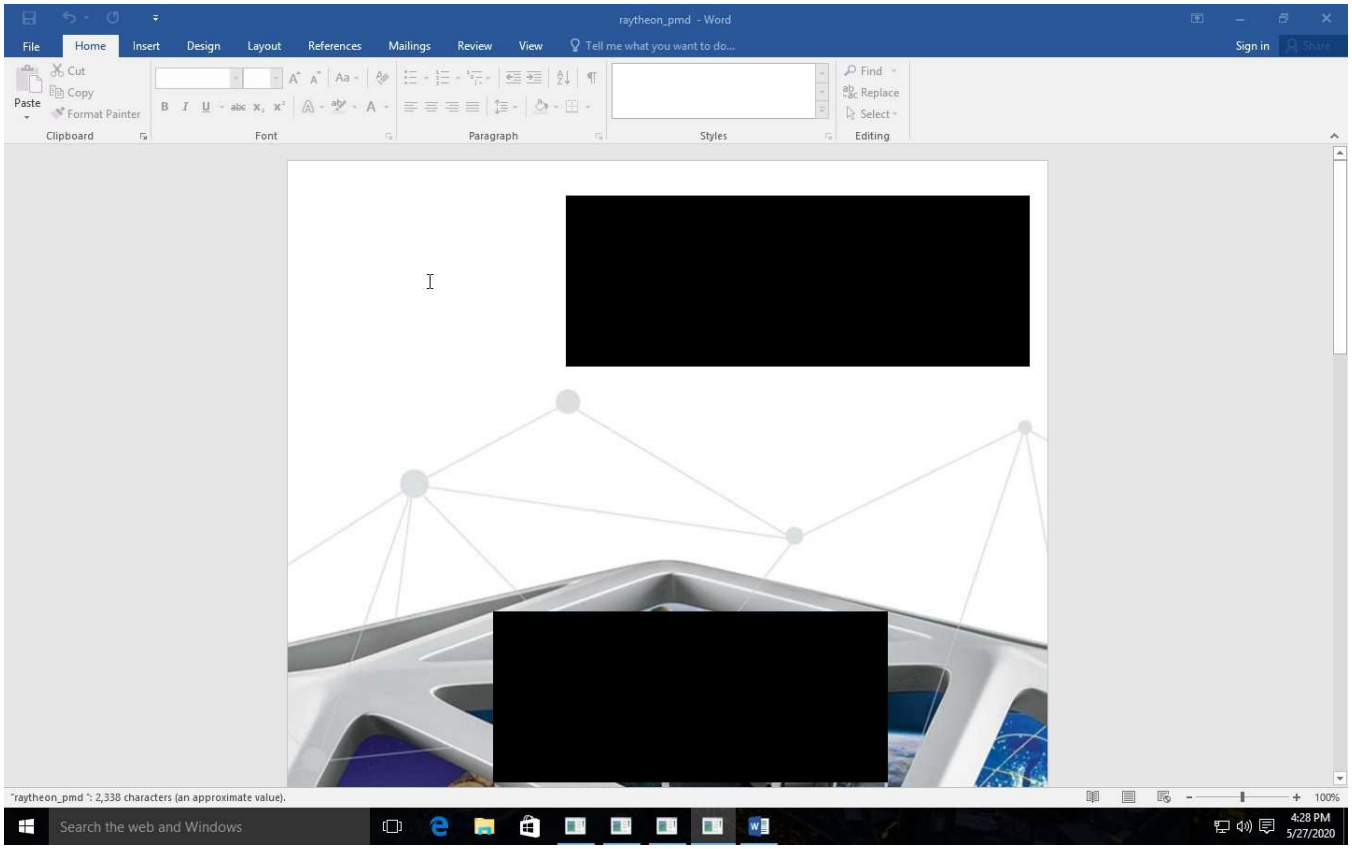
Threat Vector – Email

The screenshot below is of the phishing email which linked to a drobox download page where the victim downloaded a weaponized Microsoft Word document.

GENERAL DYNAMICS

Sample Word Document Behavior and Network Information

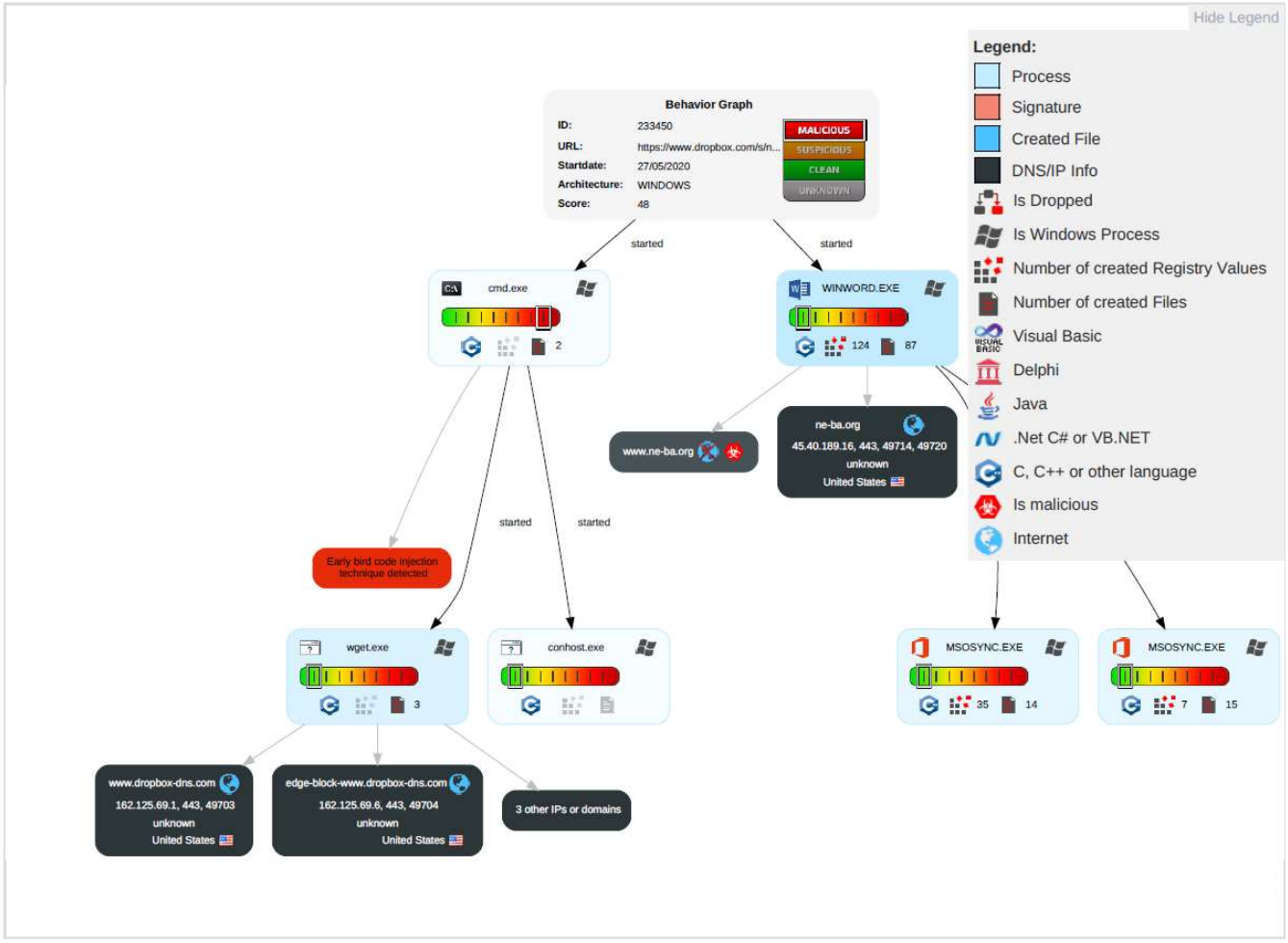
The lure documents employ template injection and Visual Basic for Applications macros to install stage one malware on a compromised host.



Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Graphical User Interface 1	Winlogon Helper DLL	Process Injection 1 1 1	Masquerading 1	Credential Dumping	Virtualization/Sandbox Evasion 1	Application Deployment Software	Data from Local System	Data Compressed	Standard Cryptographic Protocol 2	Eavesdr Insecure Network Commur
Replication Through Removable Media	Service Execution	Port Monitors	Accessibility Features	Modify Registry 1	Network Sniffing	Security Software Discovery 1 1	Remote Services	Data from Removable Media	Exfiltration Over Other Network Medium	Standard Non-Application Layer Protocol 1	Exploit S Redirect Calls/SM
External Remote Services	Windows Management Instrumentation	Accessibility Features	Path Interception	Virtualization/Sandbox Evasion 1	Input Capture	System Information Discovery 1 2	Windows Remote Management	Data from Network Shared Drive	Automated Exfiltration	Standard Application Layer Protocol 2	Exploit S Track De Location
Drive-by Compromise	Scheduled Task	System Firmware	DLL Search Order Hijacking	Process Injection 1 1 1	Credentials in Files	System Network Configuration Discovery	Logon Scripts	Input Capture	Data Encrypted	Multiband Communication	SIM Card Swap

GENERAL DYNAMICS



GENERAL DYNAMICS

Conclusion

While it is unlikely that any further activity was successfully conducted by the threat actor beyond initial infection, the customer SOC continues to monitor the environment for all known APT 38 IOCs delivered thru automated means from the GD-ISAC Threat Intel Platform (TIP). Even scenarios where APTs gain a small foothold can lead a residual and persistent presence if proper remediating steps are not taken. At this time customer has no evidence of any residual traces of the threat actor. The likely identity of the threat actor was ascertained from IOCs provided thru the GD-ISAC TIP, and confirmed by the virus total submission behavior information from a Private Industry group report

How We Stop The Threat:

The GD-ISAC works with multiple government agencies and private industry partner groups to push and pull high confidence indicators and compare them with Open source IOCs. These IOCs are curated from some of the most advanced collection platforms that monitor the internet for commonly used virus submission websites as well as unclassified reporting sources, forms, paste dump sites, dark websites, and special access forums. The IOCs are then consolidated within the GD-ISACs award winning TIP SOAR platform and enriched with additional analysis and context and pushed to the customer’s security appliances. This process ensures that the organization is always up to date with current IOCs, intelligence reports, and can actively engage the customer with the most up to date information.