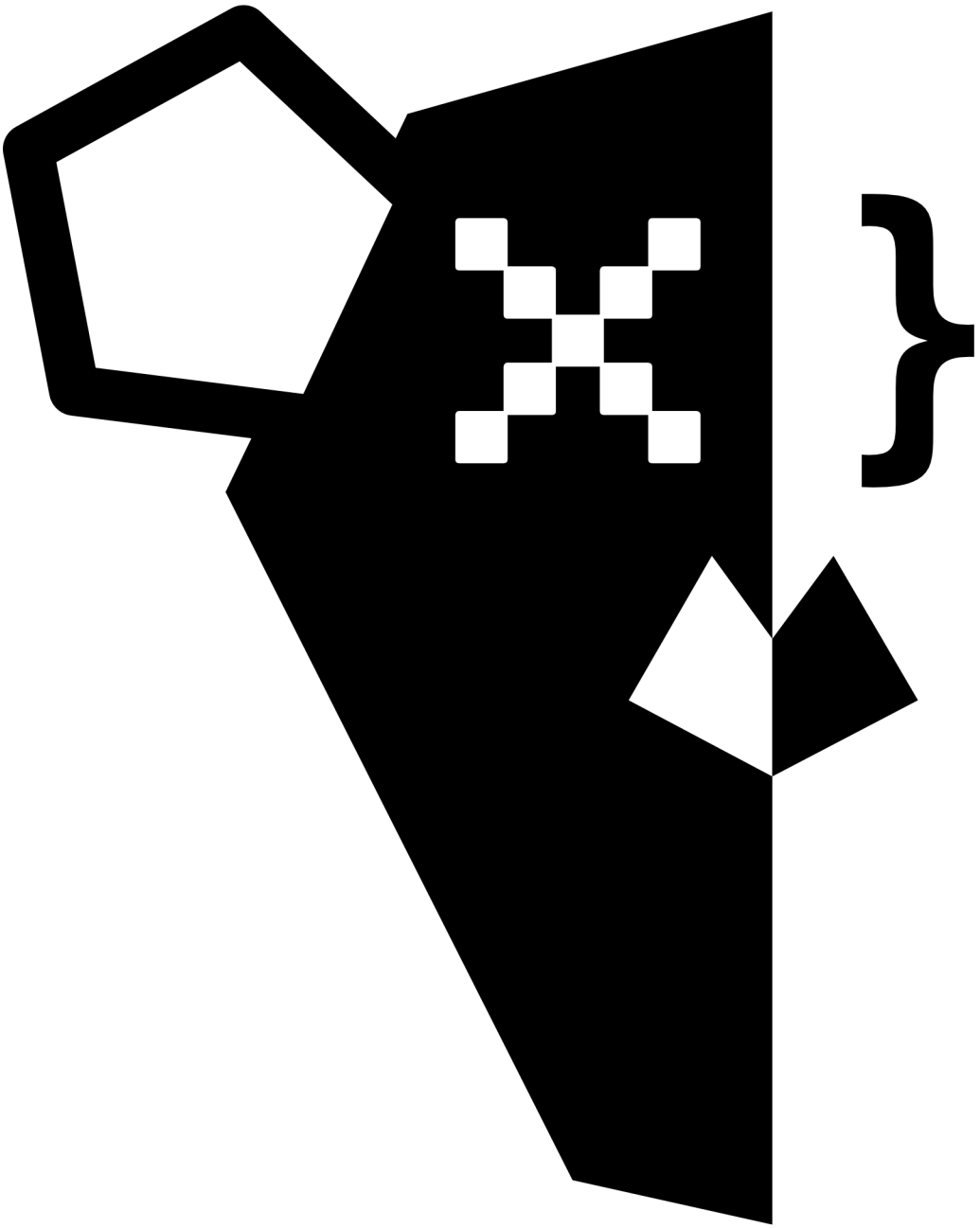

APT41

executive summary

APT41 is a Chinese state sponsored cyber espionage group known under the alias {wicked panda} that simlultaneaously conducts financially motivated operations of their own volition. wicked panda is most well known for targeting virtual currency markets, including in-game currencies for massively multiplayer online enviornments. APT41 has been active since 2012 and has since broadened it's scope of industry to healthcare and telecom, as well as more general technology fields. Most often, they operate on gaming focused targets within the 06:00pm to 07:00am time window. Considering Goodcorp's plan to spin up Gamecorp and launch a competitor to DOTA and get involved in more eSports related titles, it is reasonable for us to conclude that APT41 is a threat to Goodcorp.

One method APT41 has used repeatedly to gain access to a network is spearphishing. This could take place within Gamecorp if a well designed spearphishing campaign was used to target a lead developer and convinced them to download a malicious file. The now compromised, insecure system can be manipulated remotely and act with what would appear as trusted credentials on our network. this makes it easy for malicious actions like file exfiltration or deletion to take place, and poses severe risk to current and future daily business operations. Spearphishing itself isn't something we can stop from occurring, however, there are ways we can strengthen the network group policy and mitigate the damage that a successful spearphishing campaign could cause.

We already have mitigated a number of commonly known vulnerabilities that APT41 is likely to exploit on Gamecorp. This work was done elsewhere in the corporation within our travel industry division. This was achieved by fortifying our network against another threat actor, APT39. APT39 targets mainly travel and telecommunications sectors, and at this time are not a direct threat to Gamecorp. However, APT39 and APT41 share a number of techniques, tactics, and procedures, and work we have already done in the afforementioned travel division of Goodcorp can be used to bolster our defenses against APT41 within Gamecorp. This report lays out an explanation of APT41's tactics, techniques, and procedures, aided by documentation from NIST and MITRE ATT&CK, as well as our defenses for them. Here's a summarized overview of our areas of focus regarding some commonly exploited microsoft office vulnerabilities:

CVE-2012-0158 \ a vulnerability in MSCOMCTL.OCX in Microsoft Office and some other Microsoft products. A remote code execution vulnerability exists in the Windows common controls. An attacker could exploit the vulnerability by constructing a specially crafted webpage. When a user views the webpage, the vulnerability could allow remote code execution. patched by microsoft in 2012 so we should ensure we've kept our software up to date so this doesnt become part of our attack surface.

CVE-2015-1641 \ a remote code execution vulnerability that exists in Microsoft Office software when it fails to properly handle rich text format files in memory. If the current user is logged on with administrative user rights, an attacker could take control of the affected system. An attacker could then install programs, view, change or delete data, or create new accounts with full user rights. In April 2015, microsoft released a security update that changes the way office handles files in memory to patch this vulnerability

CVE-2017-0199 \ remote code execution vulnerability that exploits the way Microsoft Office and WordPad parse a specially written file. Exploitation can lead to full control of the affected system. Patched by microsoft in april 2017 update to Office and WordPad

CVE-2017-11882 \ a memory corruption vulnerability in Microsoft Office's Equation Editor that enables remote code execution on vulnerable devices. microsoft released a patch for this vulnerability as part of their November Patch Tuesday release in 2017.

CVE-2019-3396 \ a critical server-side template injection vulnerability in CSDCWC that can lead to path traversal and remote code excecution. used specifically by APT41 to deliver crypto mining malware paired with a rootkit designed to hide activity. Atlassian released a software patch to fix the vulnerability CVE-2019-33961. Confluence Server and Confluence Data Center versions 6.15.1, 6.14.2, 6.13.3, 6.12.3, and 6.6.12 (and any

APT41 \\ wicked_panda

APT41, or wicked panda is most well known for targeting virtual currency markets, including in-game currencies for massively multiplayer online enviornments. APT41 has been active since 2012 and has since broadened it's scope of industry to healthcare and telecom, as well as more general technology fields. Most often, they operate on gaming focused targets within the 06:00pm to 07:00am time window. here's an overlook of how APT41 and APT39's attack lifecycle compare and contrast:

Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access
Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpret	Account Manipulation	Abuse Elevation Control Mechani	Abuse Elevation Control Mechani	Adversary-in-the-Middle
Compromise Accounts	Exploit Public-Facing Application	Container Administration Comma	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force
Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Autostart Executio	Boot or Logon Autostart Executio	BITS Jobs	Credentials from Password Store
Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scrip	Boot or Logon Initialization Scrip	Build Image on Host	Exploitation for Credential Acces
Establish Accounts	Phishing	Inter-Process Communication	Browser Extensions	Create or Modify System Process	Debugger Evasion	Forced Authentication
Obtain Capabilities	Replication Through Removable	Native API	Compromise Client Software Bina	Domain Policy Modification	Deobfuscate/Decode Files or Inf	Forge Web Credentials
Stage Capabilities	Supply Chain Compromise	Scheduled Task/Job	Create Account	Escape to Host	Deploy Container	Input Capture
s	Trusted Relationship	Serverless Execution	Create or Modify System Process	Event Triggered Execution	Direct Volume Access	Modify Authentication Process
	Valid Accounts	Shared Modules	Event Triggered Execution	Exploitation for Privilege Escalati	Domain Policy Modification	Multi-Factor Authentication Inter
		Software Deployment Tools	External Remote Services	Hijack Execution Flow	Execution Guardrails	Multi-Factor Authentication Requ
		System Services	Hijack Execution Flow	Process Injection	Exploitation for Defense Evasion	Network Sniffing
		User Execution	Implant Internal Image	Scheduled Task/Job	File and Directory Permissions M	OS Credential Dumping
		Windows Management Instrume	Modify Authentication Process	Valid Accounts	Hide Artifacts	Steal Application Access Token
			Office Application Startup		Hijack Execution Flow	Steal or Forge Authentication Cer
			Pre-OS Boot		Impair Defenses	Steal or Forge Kerberos Tickets
			Scheduled Task/Job		Indicator Removal	Steal Web Session Cookie
			Server Software Component		Indirect Command Execution	Unsecured Credentials
			Traffic Signaling		Masquerading	
			Valid Accounts		Modify Authentication Process	
					Modify Cloud Compute Infrastructure	
					Modify Registry	
					Modify System Image	
					Network Boundary Bridging	
					Obfuscated Files or Information	
					Plist File Modification	
					Pre-OS Boot	
					Process Injection	
					Reflective Code Loading	
					Rogue Domain Controller	
					Rootkit	
					Subvert Trust Controls	
					System Binary Proxy Execution	
					System Script Proxy Execution	
					Template Injection	
					Traffic Signaling	
					Trusted Developer Utilities Proxy Execution	
					Unused/Unsupported Cloud Regions	
					Use Alternate Authentication Material	
					Valid Accounts	
					Virtualization/Sandbox Evasion	
					Weaken Encryption	
					XSL Script Processing	

Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Remova	Data Transfer Size Limits	Data Destruction
Credentials from Password Store	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding	Exfiltration Over Alternative Proto	Data Encrypted for Impact
Exploitation for Credential Acces	Cloud Infrastructure Discovery	Remote Service Session Hijackin	Automated Collection	Data Obfuscation	Exfiltration Over C2 Channel	Data Manipulation
Forced Authentication	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Dynamic Resolution	Exfiltration Over Other Network M	Defacement
Forge Web Credentials	Cloud Service Discovery	Replication Through Removable	Clipboard Data	Encrypted Channel	Exfiltration Over Physical Medium	Disk Wipe
Input Capture	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service	Endpoint Denial of Service
Modify Authentication Process	Container and Resource Discover	Taint Shared Content	Data from Configuration Reposit	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Multi-Factor Authentication Inter	Debugger Evasion	Use Alternate Authentication Ma	Data from Information Repositor	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Multi-Factor Authentication Requ	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service
Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
OS Credential Dumping	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
Steal Application Access Token	Network Service Discovery		Data Staged	Proxy		System Shutdown/Reboot
Steal or Forge Authentication Cer	Network Share Discovery		Email Collection	Remote Access Software		
Steal or Forge Kerberos Tickets	Network Sniffing		Input Capture	Traffic Signaling		
Steal Web Session Cookie	Password Policy Discovery		Screen Capture	Web Service		
Unsecured Credentials	Peripheral Device Discovery		Video Capture			
	Permission Groups Discovery					
	Process Discovery					
ure	Query Registry					
	Remote System Discovery					
	Software Discovery					
	System Information Discovery					
	System Location Discovery					
	System Network Configuration Discovery					
	System Network Connections Discovery					
	System Owner/User Discovery					
	System Service Discovery					
	System Time Discovery					
	Virtualization/Sandbox Evasion					
Execution						
ons						
terial						

Something that stands out here is both APT's reliance on the use of verified accounts within a network from initial compromise all the way up until the credential access stage. This means our own trusted users are our largest attack surface and should be taken into consideration when planning mitigations as its likely that heavily fortifying our own user and group policy is the best shot at stopping an attack before it can reach credential access or discovery stages.

APT41 \\ TTPS

> abuse of BITS jobs

- both APT 39 and APT41 are known to abuse BITS jobs to persistently execute code and perform various background tasks. Windows Background Intelligent Transfer Service (BITS) is a file transfer mechanism exposed through Component Object Model (COM). COM is a component of the native Windows API that enables interaction between software objects, or executable code that implements one or more interfaces.Through COM, a client object can call methods of server objects, which are typically binary DLLs or executables.

mitigation \ detection

\\\ Modify network and/or host firewall rules, as well as other network controls, to only allow legitimate BITS traffic

\\\ Consider reducing the default BITS job lifetime in Group Policy or by editing:

JobInactivityTimeout and MaxDownloadTime Registry values in:

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\BITS

\\\ Monitor for newly constructed network activity generated by BITS. BITS jobs use HTTP(S) and SMB for remote connections and are tethered to the creating user and will only function when that user is logged on

> boot \ logon autostart execution

- APT41 may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.

mitigation \ detection

\\\! This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of system features.

the best form of mitigation for this technique is detecting and nullifying it as quickly as possible. we can do that by:

\\\ Monitor DLL loads by processes, specifically looking for DLLs that are not recognized or not normally loaded into a process.

\\\ Monitor for newly constructed files that may configure system settings to automatically execute a program during system boot or logon

\\\ Monitor for changes made to files that may configure system settings to automatically execute a program during system boot or logon

\\\ Monitor for additions / changes to mechanisms that could be used to trigger autostart execution, such as relevant additions to the Registry.

APT41 \\ TTPS_01

> utilization of cobalt strike

- because cobalt strike is relatively easy to get onto an unsecure system, and due to the numerous features its able to exploit once its on a victim machine based on commands from its C2 server, its difficult to fully mitigate or even detect cobalt strike within a network. A few things we can do to have the best shot against cobalt strike would be TLSI, SSL fingerprinting, and keeping a close eye on popular services within the network.

mitigation \ detection:

\\\ TLSI <transport_layer_security_inspection>

- a security mechanism that allows enterprises to decrypt traffic, inspect the decrypted content for threats, and then re-encrypt the traffic before it enters or leaves the network. This enhances visibility within boundary security products but introduces new risks. One risk is improper control of decrypted traffic. Once traffic is decrypted, if it is sent to another host for inspection (such as an external server), there is a risk that the traffic will be mishandled. There's also a risk of Certificate Authority Compromise in addition to the issue of creating a single point of failure within the network. Additionally, there's a risk of insider access to decrypted traffic, and the possibility that the afformentioned insider is malicious.

\\\ keep an eye on popular services. After exploiting a vulnerability, Cobalt Strike usually emulates a frequently used service so it can never be detected. Running scans validated by a known trusted copy of the popular binary can help ensure our commonly used services are not being exploited by cobalt strike.

\\\ SSL fingerprinting is a technique that associates an application and/or TLS library with parameters extracted from a TLS ClientHello by using a database of curated fingerprints this can be useful for detecting Cobalt Strike because it ships with a default SSL certificate for HTTPS communication2. By identifying this default certificate, we can detect and track cobalt strike activity within our network

While some aspects of cobalt strike are able to be mitigated using protocols already in place against APT39 and both groups use C2 servers as a form of remote communcation or exfiltration, APT39 uses HTTP in C2 comms, while APT41 uses DNS traffic instead, so our network filtering will need to be adjusted accordingly to capture C2 communcations related to APT41

> abuse of windows credential editor / LSASS dumping

- APT41 is known to prefer using windows credential editor to dump password hashes from memory. they will use mimikatz to perform the same function, but their preference is generally credential editor

\\\ Manage the access control list for "Replicating Directory Changes" and other permissions associated with domain controller replication.

\\\ Add users to "Protected Users" Active Directory Security Group to limit the caching of plaintext user credentials

\\\ On Windows 10, enable Attack Surface Reduction <ASR> rules to secure LSASS and prevent credential stealing

\\\ Linux:Scraping the passwords from memory requires root privileges. Follow best practices in restricting access to privileged accounts to avoid hostile programs from accessing such sensitive regions of memory.

APT41 \\ TTPS_02

> use of teamviewer as an entry point

- spearphishing campaign is successfully able to deliver a malicious attachment which ultimately uses a teamviewer_backdoor DLL to execute a malicious binary

mitigation \ detection:
\\\ yara rule for blocking a Teamviewer_backdoor:

```
rule "Teamviewer_backdoor
{
meta:
date='2019-04-14'
description='detects malicious teamviewer DLLS

strings

// PostMessageWhookfunction
$x1 = {55 8b ec 8b 45 0c 3d 12 01 00 00 75 05 83 c8 ff eb
12 8b 55 14 52 8b 55 10 52 50 8b 45 08 50 e8}

condition
uint16(0) == 0x5a4d and $x1
}
```

\\\ Block unknown or unused attachments by default that should not be transmitted over email as a best practice to prevent some vectors, such as .scr, .exe, .pif, .cpl, etc. Some email scanning devices can open and analyze compressed and encrypted formats, such as zip and rar that may be used to conceal malicious attachments.

\\\ Having a strong email authentication mechanism that enforces a strict sender domain using SPF and message integrity with DKIM. these combine to form our organizations DMARC that can be used inter-division

\\\ Monitor and analyze SSL/TLS traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows

\\\ monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)

\\\ Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed

\\\ block compiled <.chm> attachements from unknown sources, as APT41 is known for commonly using this format in their attacks

APT41 \\ reccomendations

> some final notes

\ known to use and rely on their cobalt strike beacon

\ known to exploit sticky keys vulnerabilities

\ uses C:\windows\temp often as a staging area

\ masquerades as common antivirus:

- Kasparsky.net

- macfee.ga

- symanteclabs.com

\ known to prefer windows credential editor

\ known to target trusted users within the network the most

\ known to dump LSASS memory as a means of lateral movement within a network

\ has enumerated IP addresses of network resources and used the netstat command as part of network reconnaissance. The group has also used a malware variant, HIGHNOON, to enumerate active RDP sessions.

\ makes use of mimikatz, procdump, and BITS processes to enumerate and dump LSASS memory data

\ relies on the abuse of a malicious teamviewer dll in the initial stages of their attack

\ while APT39 doesnt often leave any impact on the network they target, APT41 is known for encrypting sensitive data or even the whole network tree on their way out, so if we are compromised we should have strong, stable, and secure backups to minimize downtime

> next steps

At this time the security team reccomends implementing at the very least all the patches to resolve the CVE's noted at the beginning of this report, as simple good software hygiene can help us avoid ever dealing with a problem like APT41 or APT39. In terms of defense against APT41 specifically, we should focus on our group policy in regards to our Active Directory configuration the most, as this is where many threat actors including APT41 are able to find a weak spot within a network and begin to move laterally until theyre able to gain further access or cause damage to important company assets. This further access can be mitigated and detected by implementing the OS/network protocol controls mentioned throughout the report. we reccomend implementing the yara rule in our IDS that blocks the malicious teamviewer backdoor as this can shut down the APT's progress quickly. A final area of focus would be imporvements to our DMARC in regards to email security and integrity, which can help prevent a spearphishing campaign from becoming successful and leading to network breach.

end.