Earth Krahang Exploits Intergovernmental Trust to Launch Cross-Government Attacks

By By: Joseph C Chen, Daniel Lunghi Mar 18, 2024 Read time: 12 min (3285 words)

Published: 2024-03-18 · Archived: 2026-04-05 13:33:50 UTC

Introduction

Since early 2022, we have been monitoring an APT campaign that targets several government entities worldwide, with a strong focus in Southeast Asia, but also seen targeting Europe, America, and Africa. The threat actor exploits public-facing servers and sends spear phishing emails to deliver previously unseen backdoors.

Our research allowed us to identify the campaign's multiple connections with a China-nexus threat actor we track as Earth Lusca. However, since the campaign employs independent infrastructure and unique backdoors, we believe it to be a separate intrusion set that we named Earth Krahang. We will examine these connections, as well as potential links to a Chinese company named I-Soon, in a separate section.

One of the threat actor's favorite tactics involves using its malicious access to government infrastructure to attack other government entities, abusing the infrastructure to host malicious payloads, proxy attack traffic, and send spear-phishing emails to government-related targets using compromised government email accounts. Earth Krahang also uses other tactics, such as building VPN servers on compromised public-facing servers to establish access into the private network of victims and performing brute-force attacks to obtain email credentials. These credentials are then used to exfiltrate victim emails, with the group's ultimate goal being cyberespionage.

Due to mistakes on the attacker's side, we managed to retrieve multiple files from Earth Krahang's servers, including samples, configuration files, and log files from its attack tools. Combining this information with our telemetry helped us understand the Earth Krahang operation and build a clear view of the threat actor's victimology and interests. In addition, we will also share their preferred malware families and post-exploitation tools in this report.

Reconnaissance and initial access

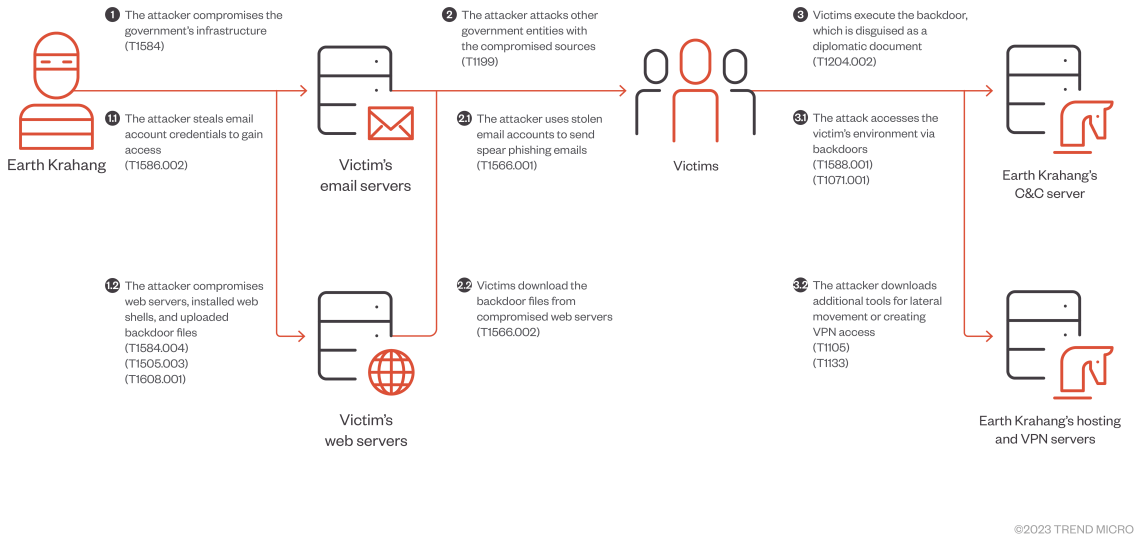

Figure 1. Infection chain of an Earth Krahang's spear-phishing attack (see the MITRE ATT&CK section for the details of each technique ID)

One of the infection vectors used involves the scanning of public-facing servers. Earth Krahang heavily employs open-source scanning tools that perform recursive searches of folders such as *.git* or *.idea*. The threat actor also resorts to simply brute-forcing directories to help identify files that may contain sensitive information such as file paths or passwords on the victim's servers. They also tend to examine the subdomains of their targets to find interesting and possible unmaintained servers. Earth Krahang also conducts vulnerability scanning with tools like *sqlmap*, *nuclei*, *xray*, *vscan*, *pocsuite*, and *wordpressscan* to find web server vulnerabilities that will allow them to access the server, drop web shells, and install backdoors.

The threat actor abused the following vulnerabilities multiple times:

- CVE-2023-32315open on a new tab: command execution on OpenFire
- CVE-2022-21587open on a new tab: command execution on Oracle Web Applications Desktop Integrator

Earth Krahang also makes use of spear phishing email to attack its targets. Like most spear phishing attacks, the emails are intended trick their targets into opening attachments or embedded URL links that ultimately lead to the execution of a prepared backdoor file on the victim's machine. Our telemetry data and some of the group's backdoors uploaded on VirusTotal revealed that the backdoor filenames are usually related to geopolitical topics, indicating their preferred type of lure:

- *"Plan of Action (POA) - TH-VN - TH_Counterdraft_as of Feb 2022.doc.exe"*
- *คำบอกกล่าวคำฟ้อง.rar*
  (translated as *"Notice of complaint.rar"*)
- *"ร่างสถานะ ครม. รว. ไทย-โรมาเนีย as of 25 Feb 2022.doc.exe"*
  (translated as *"Draft Cabinet status of Thailand-Romania as of 25 Feb 2022.doc.exe")*
- *"Malaysian defense minister visits Hungary.Malaysian defense minister visits Hungary.exe"*
- *"ICJ public hearings- Guyana vs. Venezuela.ICJ public hearings- Guyana vs. Venezuela.exe"*
- *"On the visit of Paraguayan Foreign Minister to Turkmenistan.exe"*
- *"pay-slip run persal payslip.pay-slip run persal payslip.docx.exe"*

We noticed that Earth Krahang retrieves hundreds of email addresses from their targets during the reconnaissance phase. In one case, the actor used a compromised mailbox from a government entity to send a malicious attachment to 796 email addresses belonging to the same entity. The malicious attachment was a RAR archive containing an LNK file that deployed the Xdealer malware (which we will discuss in the *Delivered malware families* section) and opened a decoy document (available online) related to the governmental entity. It is likely that the actor discovered the weak credentials of the compromised mailbox using brute-forcing tools.

Earth Krahang abuses the trust between governments to conduct their attacks. We found that the group frequently uses compromised government webservers to host their backdoors and send download links to other government entities via spear phishing emails. Since the malicious link uses a legitimate government domain of the compromised server, it will appear less suspicious to targets and may even bypass some domain blacklists.

In addition, the actor used a compromised government email account to send email to other governments. We noticed the following email subjects being used for spear-phishing emails:

- salary
- Malaysian Ministry of Defense Circular
- Malaysian defense minister visits Hungary
- ICJ public hearings- Guyana vs. Venezuela
- About Guyana Procurement Proposal for Taiwan <redacted>

```
# 输入Exchange服务器的URL、用户名和密码
credentials = Credentials(username=          , password=            )
config = Configuration(server=                   , credentials=credentials, auth_type=NTLM)

# 创建Exchange账户对象
account = Account(primary_smtp_address=                    , credentials=credentials, autodiscover=False, config=config)

f = open(        ,"r")
lines = f.readlines()
count = 0
for line in lines:
    count += 100
    # 构造电子邮件对象
    to_recipients = [Mailbox(email_address=line.strip())]
    subject = "Malaysian Ministry of Defense Circular"
    guid = str(uuid.uuid1().hex)
    body = "Kyrgyzstan criminals fled to Malaysia, check the details::https://                /data/frontend/hu/index.php?id="+guid
    message = Message(account=account, subject=subject, body=body, to_recipients=to_recipients)
    # 发送电子邮件
    message.send()
    content_tz = line.strip()+"    "+body
    print(line.strip()+':邮件发送成功')
```

Figure 2. The Python script used by Earth Krahang to send spear-phishing emails to other governments via a stolen government account (redacted)

Our telemetry also showed that the threat actor compromised a government web server and leveraged it to scan vulnerabilities in other government targets.

Post-exploitation TTPs

The threat actor installs the SoftEtheropen on a new tab VPN on compromised public-facing servers and uses *certutil* commands to download and install the SoftEther VPN server. The SoftEther server executable is renamed to either *taskllst.exe*, *tasklist.exe*, or *tasklist_32.exe for* the Windows executable and *curl* for the Linux executable

to make it look like a legitimate file on the installed system. With the VPN server installed, the actor can then connect to the victim's network to conduct their post-exploitation movements.

Additional post-exploitation movements include:

- Maintaining backdoor persistence with task scheduling
- Enabling Remote Desktop connections by modifying the Windows Registry "fDenyTSConnections"
- Accessing credentials by dumping Local Security Authority Subsystem Service (LSASS) with Mimikatz or ProcDump
- Accessing credentials by dumping the SAM database (*HKLM/sam*) from the Windows Registry
- Scanning the network using Fscan
- Lateral code execution via WMIC
- Using tools such as BadPotato, SweetPotato, GodPotato, or PrinterNotifyPotato for privilege escalation on Windows systems
- Exploiting CVE-2021-4034, CVE-2021-22555, and CVE-2016-5195 for privilege escalation on Linux systems

Email exfiltration

We observed Earth Krahang conducting brute force attacks on Exchange servers via their Outlook on the web (formerly known as Outlook Web Access, or OWA) portals of its victims. The threat uses a list of common passwords to test the email accounts on the target's email server. We have observed the group using a custom Python script targeting the ActiveSync service on the OWA server to perform their brute-force attack.

We also found the threat actor using the open-source tool *ruler*open on a new tab to brute force email accounts and passwords. Email accounts using weak passwords can be identified by the attacker, who can then perform email exfiltration or abuse the compromised account to send spear phishing emails (as we discussed earlier).

We also identified another Python script that the actor used to exfiltrate emails from a Zimbra mail server. The script can package the victim's mailbox via the mail server API using an authenticated cookie stolen by the threat actor. However, our investigation was unable to determine how the authenticated tokens were stolen from the victim's server.

```python
def getFile(email, cookies):

    headers = {
    'Host':                 ,
    'User-Agent': 'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:102.0) Gecko/251000 Firefox/102.0',
    'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8',
    'Accept-Language': 'en-US,en;q=0.5',
    'Accept-Encoding': 'gzip, deflate',
    'Cookie': "ZM_AUTH_TOKEN="+cookies
    }
    url = "https://              /service/home/%s?fmt=tgz&query=after:%s"%(email,times)
    resp = requests.get(url, stream=True, headers=headers,verify=False)
    total = int(resp.headers.get('content-length', 0))
    fname = email
    with open(fname, 'wb') as file, tqdm(
        desc=fname,
        total=total,
        unit='iB',
        unit_scale=True,
        unit_divisor=1024,
    ) as bar:
        for data in resp.iter_content(chunk_size=1024):
            size = file.write(data)
            bar.update(size)
```

Figure 3. The Python script used by Earth Krahang to exfiltrate the victim's mailbox

Delivered malware families

Earth Krahang delivers backdoors to establish access to victim machines. Cobalt Strike and two custom backdoors, RESHELL and XDealer, were employed during the initial stage of attack. We found that these backdoors were delivered either through spear-phishing emails or deployed via web shell on compromised servers.

We found the RESHELL backdoor being used several times in attacks during 2022. It was mentioned being used in a targeted attack against a Southeast Asian government by Palo Alto in a previous research reportopen on a new tab. RESHELL is a simple .NET backdoor that possesses the basic capabilities of collecting information, dropping files, or executing system commands. Its binaries are packed with ConfuserEX and its command-and-control (C&C) communication is encrypted with the AES algorithm.

Since 2023, the Earth Krahang shifted to another backdoor (named XDealer by TeamT5open on a new tab and DinodasRATopen on a new tab by ESET). Compared to RESHELL, XDealer provides more comprehensive backdoor capabilities. In addition, we found that the threat actor employed both Windows and Linux versions of XDealer to target different systems.

Each XDealer sample embeds a mark string that represents the backdoor's version. We observed the following marks:

Mark	First seen`	Platform
Win_%s_%s_%u_V10	2023-09	Windows
Din_%s_%s_%u_V12	2023-04	Windows
Din_%s_%s_%u_V10	2023-04	Windows
Linux_%s_%s_%u_V10	2023-01	Linux

Win_%s_%s_%u_V6	2022-10	Windows
Din_%s_%s_%u_V1	2022-09	Windows
Rin_%s_%s_%u_V6	2021-04	Windows

Table 1. The list of the identified marks embedded on XDealer samples

This finding indicates that the backdoor may have been used in the wild for some time now and is still under active development.

It's worth noting that many early XDealer samples were developed as a DLL file packaged with an installer, a stealer module DLL, a text file contents ID string, and an LNK file. The LNK file executes the installer, which then installs the XDealer DLL and the stealer module DLL on the victim’s machine. The stealer module can take screenshots, steal clipboard data, and log keystrokes.

In one case, we found that the LNK file was replaced with another executable, which is an installer loader (it’s likely that Earth Krahang employed a different execution scheme instead of a standalone executable). Furthermore, we found that some of the XDealer DLL loaders were signed with valid code signing certificates issued by GlobalSign to two Chinese companies. According to public information available on the internet, one is a human resource company, while the other is a game development company. It’s likely that their certificates were stolen and abused to sign malicious executables.

Package name	**Installer**	**XDealer DLL**	**Screenshot module DLL**	**ID file**	**LNK/Loader**
GoogleVaS	RuntimeInit.exe	1.dll	2.dll	id.data	RuntimeInit.lnk
GoogleUps	GoogleUpdate.exe	1.dll	2.dll	Id.data	GoogleUpdate.lnk
GoogleInc	GoogleUpdate.exe	twain_64.dll	advapi64.dll	-	svrhost.exe

Table 2. The list of packages delivering XDealer DLL and other files

Certificate hash	**Certificate**
be9de0d818b4096d80ce7d88110917b2a4e8273f	上海笑聘网络科技有限公司
be31e841820586e9106407d78ae190915f2c012d	上海指聚网络科技有限公司

Table 3. The list of certificates abused to sign the XDealer loader

Cobalt Strike was also frequently used during the initial stage of an attack. Interestingly, we found that instead of the typical Cobalt Strike usage, Earth Krahang adds additional protection to their C&C server through the adoption of the open-source project RedGuardopen on a new tab, which is basically a proxy that helps red teams hinder the discovery of their Cobalt Strike C&C profile.

The threat actor abused RedGuard to prevent its C&C servers from being identified by blue team Cobalt Strike C&C scanners or search engine web crawlers. It also helps the group monitor who is collecting their C&C profiles. We found that Earth Krahang's C&C server redirected invalid C&C requests to security vendor websites due to RedGuard's protections.

Cobalt Strike exploits the DLL side-loading vulnerability. In one case we analyzed, the threat actor dropped three files, *fontsets.exe*, *faultrep.dll*, and *faultrep.dat*. The file *fontsets.exe* (SHA256: 97c668912c29b8203a7c3bd7d5d690d5c4e5da53) is a legitimate executable that was abused to side-load the DLL file *faultrep.dll* (SHA256: a94d0e51df6abbc4a7cfe84e36eb8f38bc011f46).

The *faultrep.dll* file is a custom shellcode loader that will decode the encoded shellcode — which is Cobalt Strike — stored inside *faultrep.dat*. We also found another DLL loader with a similar decoding routine, but with different byte values for decoding and loads shellcode from a different filename (*conf.data*).

Using our telemetry data, we found that the threat actor also dropped PlugX and ShadowPad samples in victim environments. The PlugX sample, named *fualtrep.dll*, is likely used for side-loading, similar to the Cobalt Strike routine mentioned above. The ShadowPad samples had the exact same characteristics as seen in our previous Earth Lusca report.

Victimology

We found approximately 70 different victims (organizations that were confirmed to be compromised) spread across 23 different countries. Since we had access to some of Earth Krahang's logs, we were also able to identify 116 different targets (including those that were not confirmed to be compromised) in 35 countries.

In total, the threat actor was able to compromise or target victims in 45 different countries spread across different regions, most of them in Asia and America, but also in Europe and Africa.

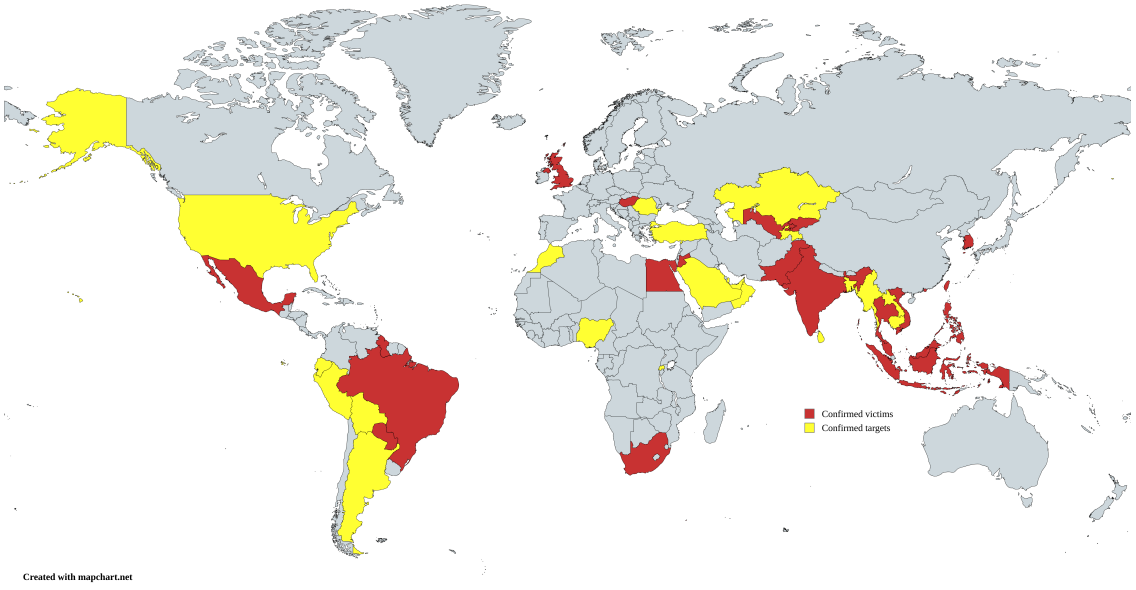

Figure 4. The map of victims targeted by Earth Krahang (countries in red are those that at least one entity compromised, while countries in yellow are those with at least one entity targeted)

Government organizations seem to be Earth Krahang's primary targets. As an example, in the case of one country, we found that the threat actor compromised a diverse range of organizations belonging to 11 different government ministries.

We found that at least 48 government organizations were compromised, with a further 49 other government entities being targeted. Foreign Affairs ministries and departments were a top target, compromising 10 such organizations and targeting five others.

Education is another sector of interest to the threat actor. We found at least two different victims and 12 targets belonging to this sector. The communications industry was also targeted; we found multiple compromised telecommunications providers. Other target organizations and entities include post offices (targeted in at least three different countries), logistics platforms, and job services.

There were other industries targeted, but on a smaller scale, including the following:

- Finance/Insurance
- Foundations/NGOs/Thinkthanks
- Healthcare
- IT
- Manufacturing
- Media
- Military
- Real estate
- Retail
- Sports
- Tourism

Attribution

Initially, we had no attribution for this campaign since we found no infrastructure overlaps, and had never seen the RESHELL malware family before. Palo Alto published a reportopen on a new tab that attributes, with moderate confidence, a particular cluster using RESHELL malware to GALLIUMopen on a new tab. However, the assessment is based on a toolset that is shared among many different threat actors, and we were hesitant to use this link for proper attribution. We also considered the possibility that RESHELL is a shared malware family.

Earth Krahang switched to the XDealer malware family in later campaigns. In a research paperopen on a new tab presented by TeamT5, XDealer was shown to be associated with Luoyuopen on a new tab, a threat actor with Chinese origins that used the WinDealeropen on a new tab and ReverseWindow malware families. Our colleague, who was previously involved in the research of Luoyu, shared with us the insights on this association, particularly the sharing of an encryption key between an old XDealer sample and a SpyDealer sample — suggesting a connection between both malware families. ESET, which named this malware DinodasRAT, wrote an extensive reportopen on a new tab on its features. However they had no particular attribution apart from the possible China-nexus origin.

While we believe it could be possible that this campaign has links to LuoYu, we found no traces of other malware families used by this threat actor. Also, the encryption key mentioned above is different from the samples we found in this campaign, meaning that this malware family has multiple builders. This could suggest that either the key was changed at some point in development, or that the tool is shared among different groups.

In January 2022, we reported on a China-nexus threat actor we called Earth Lusca, following up with updates on their use of a newly discovered backdoor named SprySOCKS and their recent activities capitalizing on the Taiwanese presidential election. During our investigation, we noticed malware being downloaded from IP addresses we attribute to Earth Lusca (45[.]32[.]33[.]17 and 207[.]148[.]75[.]122, for example) at the lateral movement stage of this campaign. This suggests a strong link between this threat actor and Earth Lusca. We also found infrastructure overlaps between some C&C servers that communicated with malware we found during our investigation, and domain names such as *googledatas[.]com* that we attribute to Earth Lusca.

While the infrastructure and the preference of the initial stage backdoors look to be very different between this new campaign and the previously reported activities of Earth Lusca, our speculation is that they are two intrusion sets running independently but targeting a similar range of victims, becoming more intertwined as they approach their goal — possibly even being managed by the same threat group. Due to these characteristics, we decided to give the independent name, Earth Krahang, to this intrusion set.

Our previous report suggests Earth Lusca might be the penetration team behind the Chinese company I-Soon, which had their information leaked on GitHub recently. Using this leaked information, we found that the company organized their penetration team into two different subgroups. This could be the possible reason why we saw two independent clusters of activities active in the wild but with limited association. Earth Krahang could be another penetration team under the same company.

Conclusion

In this report, we shared our investigation on a new campaign we named Earth Krahang. Our findings show that this threat actor focuses its efforts on government entities worldwide and abuses compromised government infrastructure to enable its malicious operations.

We were also able to identify two unique malware families used in Earth Krahang's attacks while also illustrating the larger picture involving the group's targets and malicious activities via our telemetry data and the exposed files on their servers.

Our investigation also identified multiple links between Earth Krahang and Earth Lusca. We suspected these two intrusion sets are managed by the same threat actor.

Given the importance of Earth Krahang's targets and their preference of using compromised government email accounts, we strongly advise organizations to adhere to security best practices, including educating employees and other individuals involved with the organization on how to avoid social engineering attacks, such as developing a healthy skepticism when it involves potential security issues, and developing habits such as refraining from clicking on links or opening attachments without verification from the sender. Given the threat actor's exploitation of vulnerabilities in its attacks, we also encourage organizations to update their software and systems with the latest security patches to avoid any potential compromise.

Indicators of Compromise

The indicators of compromise for this entry can be found here.

Acknowledgment

Special thanks to Leon M Chang who shared to us insights about the overlap of the TEA encryption key between XDealer and SpyDealer samples.

MITRE ATT&CK

The listed techniques are a subset of the MITRE ATT&CK listopen on a new tab.

Tactic	Technique	ID
Reconnaissance	Active Scanning: Scanning IP Blocks	T1595.001
	Active Scanning: Vulnerability Scanning	T1595.002
	Active Scanning: Wordlist Scanning	T1595.003
	Gether Victim Host Information	T1592
	Gether Victim Network Information	T1590
Resource Development	Acquire Infrastructure: Domains	T1583.001
	Acquire Infrastructure: Virtual Private Server	T1583.003
	Compromise Accounts: Email Account	T1586.002
	Compromise Infrastructure: Server	T1584.004
	Obtain Capabilities: Malware	T1588.001
	Obtain Capabilities: Code Signing Certificates	T1588.003
	Stage Capabilities: Upload Malware	T1608.001
	Stage Capabilities: Upload Tool	T1608.002
	Stage Capabilities: Link Target	T1608.005
Initial Access	Exploit Public-Facing Application	T1190
	Phishing: Spear phishing Attachment	T1566.001
	Phishing: Spear phishing Link	T1566.002
	Trusted Relationship	T1199

	Valid Accounts	T1078
Execution	Command and Scripting Interpreter: PowerShell	T1059.001
	Command and Scripting Interpreter: Windows Command Shell	T1059.003
	Command and Scripting Interpreter: Python	T1059.006
	Exploitation for Client Execution	T1203
	System Services: Service Execution	T1569.002
	User Execution: Malicious File	T1204.002
	Windows Management Instrumentation	T1047
Persistence	Create or Modify System Process: Windows Service	T1543.003
	External Remote Services	T1133
	Scheduled Task/Job: Scheduled Task	T1053.005
	Server Software Component: Web Shell	T1505.003
Privilege Escalation	Exploitation for Privilege Escalation	T1068
	Valid Accounts: Local Accounts	T1078.003
Defense Evasion	Deobfuscate/Decode Files or Information	T1140
	Hijack Execution Flow: DLL Side-Loading	T1574.002
	Impersonation	T1656
	Masquerading: Match Legitimate Name or Location	T1036.005
	Masquerading: Double File Extension	T1036.007
	Modify Registry	T1112
Credential Access	Brute Force: Password Spraying	T1110.003
	OS Credential Dumping: LSASS Memory	T1003.001
	OS Credential Dumping: Security Account Manager	T1003.002
	Steal Web Session Cookie	T1539
Discovery	Account Discovery: Local Account	T1087.001
	Account Discovery: Domain Account	T1087.002
	Permission Groups Discovery: Domain Groups	T1069.002

	Process Discovery	T1057
	System Owner/User Discovery	T1033
	System Service Discovery	T1007
Lateral Movement	Exploitation of Remote Services	T1210
	Internal Spear phishing	T1534
	Remote Services: Windows Remote Management	T1021.006
Collection	Automated Collection	T1119
	Email Collection	T1114
Command and Control	Application Layer Protocol: Web Protocols	T1071.001
	Encrypted Channel: Symmetric Cryptography	T1573
	Ingress Tool Transfer	T1105
	Protocol Tunneling	T1572
Exfiltration	Automated Exfiltration	T1020

Tags
