THREAT RESEARCH • ADVANCED PERSISTENT THREATS • 18 min read •

Deep Dive Into a BackdoorDiplomacy Attack – A Study of an Attacker's Toolkit

Martin

Martin Zugec
December 06, 2022

A China-linked cyber espionage operation targeting multiple telecom providers in the Middle East was recently discovered by Bitdefender Labs. A wide range of tools were used for this operation, both open-source and custom-built. Download the full research paper: "Cyber-Espionage in the Middle East: Investigating a New BackdoorDiplomacy Threat Actor Campaign" if you want to dive deeper. We attribute this operation to BackdoorDiplomacy, a known advanced persistent threat group (APT).

An APT is a sustained, sophisticated cyber-attack which employs a complex set of tactics, techniques, and procedures. These threat actors are often well-funded, experienced, and sponsored (or at least ignored) by the countries they are operating from. While these groups typically target high-value targets, they often leverage smaller companies that are part of the supply chain of their intended target (we wrote about this practice before in the Deep Dive into a Corporate Espionage Operation article).

Aside from the level of sophistication, another attribute that defines an ATP attack is the goal of remaining undetected for an extended period. Defense evasion used to be one of the defining attributes of APT threat actors, but other groups of threat actors have adopted the same tactic. With the rising popularity of the Ransomware-as-a-Service (RaaS) profit sharing model, ransomware threat actors require more time to prepare for an attack. Ransomware affiliates – those responsible for operationalizing the malware - use this time to collect and exfiltrate valuable data or locate information that can help them properly calculate the maximum potential ransom.

One of the most popular techniques used by ransomware affiliates to avoid detection is the living-off-the-land approach. Instead of deploying commodity malware that risks detection by modern prevention security controls, threat actors are using binaries, scripts, or libraries that are already on the target system (or can be downloaded without raising suspicion). You can find a list of binaries and their unexpected use for offensive purposes at project LOLBAS.

But cybersecurity is a never-ending game of cat and mouse. As attackers advance their techniques, businesses around the world continue to adopt effective methods to mitigate the longer dwell time of adversaries such as ransomware affiliates. Businesses are adopting detection and response capabilities, either as a service (MDR) or as a product (XDR). Modern detection and response solutions like Bitdefender XDR (see our demo) are highly effective at detecting and reporting when these benign tools are used for malicious purposes by threat actors.

While living-off-the-land remains an effective technique for ransomware affiliates – especially in environments which lack elementary detection and response capabilities - modern APT threat actors have had to up their game to stay ahead.

Detection and Response capabilities are now commonly adopted by small and mid-sized companies. Source: Bitdefender Cybersecurity Posture Survey 2022

To counter the rising popularity and effectiveness of detection and response tools, APTs use an array of customized attack tools that are designed to avoid detection. Many APT groups have a strong financial foundation with access to professional developers and security consultants. Some groups are now advancing into developing custom-made tools for targeting ICS/SCADA devices; developing more traditional malware is no challenge for them. As we have seen in the recent "Advanced Threat Protection – Enterprise" evaluation by AV-Comparatives, APT payloads are often detected only after the code is executed.

In this deep dive, we present our analysis of the recent operation by APT group BackdoorDiplomacy targeting telecom providers based in the Middle East. During this attack, threat actors deployed a range of tools, many of which were heavily customized or seemingly novel as they had not been encountered before. We share this research to help other companies to identify blind spots and increase cyber-resilience.

Anatomy of an attack

The complete anatomy of an attack, including all known indicators of compromise (IOCs), is available in the full research paper: "Cyber-Espionage in the Middle East: Investigating a New BackdoorDiplomacy Threat Actor Campaign". The following is a summary of this research. Detailed descriptions of many of the tools used during this attack are included in the full report. Since we observed modifications to the code of some of these tools during this incident, they continue to be under active development:

- Irafau Backdoor

- Quarian Backdoor
- Pinkman Agent
- Impersoni-fake-ator

Initial compromise

The initial infection vector was an instance of an Exchange server exploited via a known unpatched vulnerability [ProxyShell]() – a combination of vulnerabilities [CVE-2021-31207]() (authentication bypass), [CVE-2021-34523]() (escalation of privileges), and [CVE-2021-34473]() (remote code execution). This is one of the top 15 routinely exploited vulnerabilities ([source: CISA]()), allowing a threat actor to execute arbitrary code. Surprisingly, weaponizing well-known vulnerabilities is still an effective method for nation-state actors to compromise networks. This is a low-cost/high-value attack vector, and according to the latest [Data Breach Investigations Report](), over 30% of web application attacks are related to espionage (a significantly higher number than any other attack vector). When prioritizing your security strategy, make sure these routinely exploited vulnerabilities are handled as a top priority.

The attack started with an email, but this was not [a traditional phishing attack](). The malicious payload was included as an attachment, and once this email was received and processed by the Exchange server, the vulnerability was exploited (without anyone clicking on the attachment or even seeing the email). The subject of the email and the attachment name suggests that a public proof of concept for ProxyShell exploit was used.

After gaining access to this system, threat actors deployed two web shells on the compromised Exchange server. A web shell is a malicious shell-like interface (usually written in web development languages such as JSP, PHP…) that is used to access a web server remotely, providing a threat actor with access even after the exploited vulnerability is fixed. For this operation, two types of webshells were used: [ReGeorg](), and another [C# open-source webshell]().

Reconnaissance, credential access, and privilege escalation

After the initial foothold was established, threat actors continued with system discovery, identifying and locating other machines and file shares on the network. For initial reconnaissance, threat actors used a combination of built-in utility tools (including `hostname.exe`, `netstat.exe`, `net.exe`, and others), Active Directory discovery utilities (`ldifde.exe` and `csvde.exe`), and open-source scanners and other publicly available software (port scanner NimScan, IPv4/IPv6 scanner SoftPerfect Network Scanner, NetBIOS scanner NBTscan, and others).

Threat actors also collected information about users and groups – basic user information was extracted from the Exchange server by PowerShell (`Get-User -ResultSize Unlimited | Select-Object -Property Name`), with interest in Active Directory members of groups "Domain Admins", "Remote Desktop Users", and other custom groups.

Credentials were extracted from the registry by running the following commands:

- `reg save hklm\sam sam.hive`
- `reg save hklm\security security.hive`
- `reg save hklm\system system.hive`

To capture more credentials, threat actors enabled the Digest Authentication Protocol (WDigest) in the registry. This is a legacy protocol used in Windows Server 2003 and older operating systems that requires storing clear-text passwords in the memory. By enabling this protocol, threat actors can harvest not only password hashes, but also clear text passwords for all users authenticated against a server with this protocol enabled. Other tools for manipulating and extracting credentials were saved in `%Public%` folder, including secretsdump.py from Impacket, set_empty_pw.py (ZeroLogon), and ProcDump from Sysinternals.

For privilege escalation, threat actors used a custom tool `%LocalAppData%\VMware\t.exe`. This binary loader extracted and executed, in memory, the payload - a privilege escalation code based on vulnerability CVE-2018-8440. This is a binary loader written in the Nim programming language. Nim is not commonly used – threat actors probably chose it to avoid detection by security teams that are not familiar with this language. The new programming language produces bytecode sequences that are unknown to many detection tools, and this is one of the common tactics to help avoid detection.

Lateral movement

After collecting basic information about machines, networks, and users, threat actors improved the reconnaissance process with a custom tool **c:\windows\com\taskmgr.exe** (SHA256: `ba757a4d3560e18c198110ac2f3d610a9f4ffb378f29fd29cd91a66e2529a67c`). This tool uses a list of computers and a list of credentials obtained previously to gather more information, execute remote commands, and collect more data.

This tool is designed to work in both workgroup and domain environments and supports remote execution based on PsExec, WMI (using `wmic.exe`), or using remote Scheduled Tasks (using `at.exe`). After connecting to each of the machines defined in a local configuration file, this utility will copy a local batch script to a remote machine, execute this custom script, and download the output file with extracted information.

The script executes multiple commands, such as `tasklist /svc`, `ipconfig /all`, `ipconfig /displaydns`, `netstat -ano`, `net start`, `systeminfo`, and `net user`, `net localgroup administrators`. It also includes commands for listing the registry key for Internet settings, Run registry keys, and content of `c:\Users` directory. The output of all commands is redirected to the local file, which is then retrieved by the tool. An overview of this tool, including all the command line parameters and internal logic, are included in the full report.

The threat actors used also other tools for lateral movement, including `schtasks.exe`, standalone `psexec.exe`, sharp-`wmiexec.exe`, and `smbexec.py`.

Persistence and defense evasion

Persistence was established using multiple methods to provide threat actors with access to systems, including changed credentials, restarts, or other interruptions, for redundancy should one of their methods fail.

The first, and most obvious method to establish persistence is through registry Run keys (both `HKLM` and `HKCU`) for multiple separate executables, using registry value names like `AcroRd`, `Userinit`, `updatesrv`, `siem` or `vmnat`.

The second method involves the creation of multiple services, using the command sc.exe. Service names included `NetSvc` and `AppMgmt`.

The final method of persistence relies on the WMI event subscription. Custom namespace `root\Microsoft` is created, with an event that is triggered only during a short window after the startup (more than 5 minutes, but less than 6 minutes).

For evading defense, the threat actors used multiple loaders like the one presented in the Privilege Escalation section (`t.exe`), and VMProtect packed binaries. VMProtect is a legitimate software protection solution that includes anti-cracking functionality, such as debuggers or virtualization detection.

Other techniques include DLL sideloading (a technique that we have recently covered in "Tech Explainer | What is DLL Sideloading?" article), adding exclusions to Windows Defender, and *timestomping* (tampering with timestamps on the NTFS filesystem to hide file changes).

Data exfiltration

Although the aim of the attack is hard to establish, there are a few artifacts that suggest the intent of cyber-espionage. The first evidence is the use of PowerShell cmdlets `Get-Mailbox` and `Get-MessageTrackingLog` on the Exchange server for obtaining email content and metadata.

To exfiltrate data, another tool based on the open source sftp project was used. This tool downloaded a `rar.exe` executable, and then uploaded the archive to the same server. The RAR utility was used multiple times for compressing files such as discovery results, emails, and log files with keystrokes.

Another piece of evidence in favor of the hypothesis that we are dealing with an espionage operation is the use of a keylogger. The malicious component (`duser.dll`) was loaded by the legitimate credwiz.exe binary (one of the instances of the DLL sideloading technique). The log file generated by this keylogger is not encrypted – it contains the timestamp, the window name, and the typed keystrokes.

Finally, our research suggests that this operation was likely performed by a group specialized in cyber espionage, known as BackdoorDiplomacy. This group has previously targeted telecommunication companies and Ministries of Foreign Affairs in the Chinese sphere of interest, including the Middle East and Africa. The attribution is based on infrastructure and tactics, techniques, and procedures (TTP) common to the current operation and others known to the public. For instance, the already known IP address `43.251.105[.]139` was used. The domains `uc.ejalase[.]org` and `mci.ejalase[.]org` pointed to IP addresses that are related to other domains used in the past. One of such domains we believe is `support.vpnkerio[.]com` as there are other subdomains of `vpnkerio[.]com` connected to the mentioned threat actor.

Conclusion & recommendations

The best protection against modern cyber-attacks is a defense-in-depth architecture. Start with reducing your attack surface, focusing on patch management (not only for Windows but for all applications and internet-exposed services), and detection of misconfigurations. Read our technical brief to learn about GravityZone Patch Management solution.

The next security layer is reliable world-class prevention controls to eliminate most security incidents, using multiple layers of security, including IP/URL reputation for all endpoints, and protection against fileless attacks.

Implementing IP, domain, and URL reputation, powered by Bitdefender threat intelligence solution, is one of the most effective methods to stop automated vulnerability exploits. According to analysis in the Data Breach Investigations Report 2022, only 0.4% of the IPs that attempted RCEs were not seen in one of the previous attacks. Block bad IPs, domains, or URLs on all devices, including endpoints, and prevent a security breach in your business environment.

Finally, for the few incidents that get through your defenses, lean on security operations, either in-house or through a managed service, and leverage strong detection and response tools. Modern threat actors often spend weeks or months doing active reconnaissance on networks, generating alerts, and relying on the absence of detection and response capabilities.

Learn more about Gravityzone Extended Detection and Response (XDR).

We would like to thank Victor Vrabie, Adrian Schipor, and Cristina Vatamanu from the Bitdefender Labs team for their help with putting this report together.

TAGS

threat research

advanced persistent threats

AUTHOR

.artin Zugec

Martin Zugec

Martin is technical solutions director at Bitdefender. He is a passionate blogger and speaker, focusing on enterprise IT for over two decades. He loves travel, lived in Europe, Middle East and now residing in Florida.

View all posts

RIGHT NOW

TOP POSTS

Bitdefender Threat Debrief | October 2024

ENTERPRISE SECURITY • RANSOMWARE • BITDEFENDER THREAT DEBRIEF

Bitdefender Threat Debrief | October 2024

October 10, 2024 •

Meow, Meow Leaks, and the Chaos of Ransomware Attribution

ENTERPRISE SECURITY • RANSOMWARE • THREAT RESEARCH • THREAT INTELLIGENCE

Meow, Meow Leaks, and the Chaos of Ransomware Attribution

September 29, 2024 •

Understanding the Roles in the Ransomware-as-a-Service Ecosystem: Who's Targeting Your Data Security Gaps

ENTERPRISE SECURITY • RANSOMWARE • THREAT INTELLIGENCE

Understanding the Roles in the Ransomware-as-a-Service Ecosystem: Who's Targeting Your Data Security Gaps

September 19, 2024 •

The Importance of People in Cyber Risk Management: Incident Response Tabletop Exercises (TTX)

ENTERPRISE SECURITY

The Importance of People in Cyber Risk Management: Incident Response Tabletop Exercises (TTX)

September 17, 2024 •

FOLLOW US ON

SOCIAL MEDIA

SUBSCRIBE TO OUR

YOU MIGHT ALSO LIKE

AI in Cybersecurity: Can Automation Alone Secure Your Organization?

ENTERPRISE SECURITY • ENDPOINT PROTECTION & MANAGEMENT • MANAGED DETECTION AND RESPONSE

AI in Cybersecurity: Can Automation Alone Secur…

Paul Lupo
October 31, 2024

Critical Edge Network Devices: Patching Vulnerabilities to Block Ransomware

ENTERPRISE SECURITY • RANSOMWARE • ENDPOINT DETECTION AND RESPONSE

Critical Edge Network Devices: Patching…

Josue Ledesma
October 29, 2024

Identifying Security Gaps Using the NIST Cybersecurity Framework: Part 1

ENTERPRISE SECURITY • IT COMPLIANCE & REGULATIONS • PRIVACY AND DATA PROTECTION • ENDPOINT PROTECTION & MANAGEMENT

Identifying Security Gaps Using the NIST…

Kevin Gee
October 24, 2024