

# Analysis of Conti Leaks

March 11<sup>th</sup>, 2022

# Contents

- 1. Executive Summary ..... 3
- 2. Background ..... 3
- 3. Details of the Leak..... 4
- 4. Analysis of Chats..... 5
  - 4.1. Organizational Chart..... 6
  - 4.2. Exploits, in-house tools, and social engineering ..... 7
  - 4.3. Conti Victims..... 7
  - 4.4. Titbit..... 8
- 5. Analysis of Tutorials and Documents ..... 10
  - 5.1. Hacker’s quickstart guide ..... 10
  - 5.2. Researcher’s quickstart guide..... 11
- 6. Analysis of Tools ..... 12
  - 6.1. TrickBot..... 12
  - 6.2. Internal Tools..... 12
  - 6.3. Locker ..... 13
  - 6.4. IoCs ..... 14

# 1. Executive Summary

This briefing is the result of an analysis of the chats, tutorials and tools used by the Conti ransomware groups and leaked via the Twitter handle “**ContiLeaks**” since the end of February 2022.

The briefing presents intelligence about the group’s organization, attack techniques and victims which can help network defenders to detect and mitigate attacks from Conti and other similar ransomware groups. It does not rely on automatic translation of leaked chats (which are known to be [misleading](#)) but on analysis of the original material done by Russian-speaking researchers.

Although there has been much recent analysis of “ContiLeaks”, the new information on this report include:

- A list of Conti members and their functions, which expands on previously published analyses.
- New insights on victim organizations emerging from discussion on the group’s chat.
- In-depth discussion of their preferred attack methods, including a focus on IoT devices, RDP services and Windows Domain Controllers.

## 2. Background

Conti has been active since 2019 and is currently the most prolific ransomware gang, especially after the [arrest of REvil members](#) at the beginning of 2022. Conti was one of the most successful ransomware gangs in 2021 with more than [400 successful attacks on US and international organizations](#). Although it’s difficult to know exactly how much ransom they collected in total, a single [data source](#) tracking blockchain transactions reports more than \$50 million in payouts.

As most modern ransomware gangs, Conti adopts a [cybercrime-as-a-service approach](#) where different steps of an attack campaign are taken by actors in different groups (such as initial access brokers, operators and negotiators). The Conti ransomware developers sell their technology to affiliates, who in turn attack victims and share the paid ransom with Conti. [The group also uses extortion techniques beyond encryption, such as leaking breached data and publicly shaming their victims.](#)

Previous studies about Conti include:

- [Several detailed reports](#) of incidents describing the steps taken by attackers on victim networks over several days. These reports show the use of three main [tools: BazarLoader, Trickbot and CobaltStrike](#). [Another tool not mentioned in these reports but often associated with Conti is Emotet.](#)
- PRODAFT’s [in-depth report](#) based on open-source intelligence and information gathered directly from one of their servers. This report discusses the group’s history, including ties with the Ryuk ransomware group, their target selection, negotiation tactics, and money flow.
- An analysis of [intercepted negotiations](#) between Conti and their victims showing that final payments are well below initial requested sums, with an average of 7 rounds of negotiation leading to an average payment of around \$360,000.
- [CISA’s alert about Conti](#) detailing observed Tactics, Techniques, and Procedures (TTPs) and recently updated to include 98 new domains that are similar to others previously used by Conti.
- A “playbook” for operators [leaked in 2021](#) by a disgruntled affiliate, containing descriptions of attack tools and instructions on how to use them.

The studies above painted a picture of a group that uses a broad set of tools to target larger organizations for big payouts and that is particularly unscrupulous, having purposefully targeted [hospitals and emergency service providers](#).

However, the newly leaked information allows us to learn more about the group's functioning, victims and tools.

### 3. Details of the Leak


On February 25<sup>th</sup> 2022, one day after the start of Russia's invasion of Ukraine, the Conti team posted the following message on their website, showing full support for Russia's actions:


Two days later, on February 27<sup>th</sup>, a Twitter account with the handle "ContiLeaks" started sharing leaked material related to Conti's operation, initially including chat logs and later hacking tools. Table 1 lists the files that were leaked to the [vx-underground](#) website until March 11<sup>th</sup>.

Table 1 – List of leaked files

File name	File size	Date	Category	Description
<a href="#">Conti Chat Logs 2020.7z</a>	2417273	01-03-22 2:46	Chats	Chats from June until November 2020
<a href="#">Conti Documentation Leak.7z</a>	234714	01-03-22 5:29	Docs	Various documents such as technical guidelines and instructions for managers
<a href="#">Conti Internal Software Leak.7z</a>	3911885	01-03-22 2:57	Tools	12 git repositories of internal software used by Conti
<a href="#">Conti Jabber Chat Logs 2021 - 2022.7z</a>	1160294	02-03-22 13:10	Chats	Additional chats spanning 2021 and 2022
<a href="#">Conti Locker Leak.7z</a>	6852466	05-03-22 4:29	Tools	The ransomware component used by Conti
<a href="#">Conti Pony Leak 2016.7z</a>	62014991	01-03-22 2:51	Docs	Collection of credentials and certificates stolen from multiple organizations by the Pony malware
<a href="#">Conti Rocket Chat Leaks.7z</a>	3370574	01-03-22 2:47	Chats	Chat logs
<a href="#">Conti Screenshots December 2021.7z</a>	452894	01-03-22 2:46	Docs	Several screenshots of Cobalt strike toolkit used by Conti

#### "WARNING"

 The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructures of an enemy.

 2/25/2022

 55

 0 [ 0.00 B ]

<a href="#">Conti Toolkit Leak.7z</a>	94186791	01-03-22 2:42	Tools	Source code of Chimaera.Ngrok and Chimaera.Sugarlogic toolkits. Also contains manuals for file-and-rank employees that have been leaked earlier last year.
<a href="#">Conti Trickbot Forum Leak.7z</a>	8542211	01-03-22 2:50	Chats	Messages from the Trickbot forum.
<a href="#">Conti Trickbot Leaks.7z</a>	955850	01-03-22 6:52	Tools	Two backend components written in Erlang for data dispatcher and collection
<a href="#">Training Material Leak</a> (267-part zip file)	-	31-12-69 18:00	Docs	Educational text and video materials, as well as code examples.

Several researchers and cybersecurity companies have analyzed the leaks, including [Brian Krebs](#), who wrote a four-part analysis of the leaks focusing on the group's response to [previous breaches](#), their [internal working](#), their use of [commercial security services](#) and their dealings in [cryptocurrencies](#).

After the recent leak, Conti members [have deleted production machines and moved to other communication channels](#), but the group did not stop attacking organizations and since the beginning of March has [listed more than two dozen victims](#) on ContiNews.

## 4. Analysis of Chats

The leaked logs from the Rocket and Jabber chats span almost two years of conversation, as shown in the heatmap on Figure 1. However, most of that conversation is irrelevant for defenders.

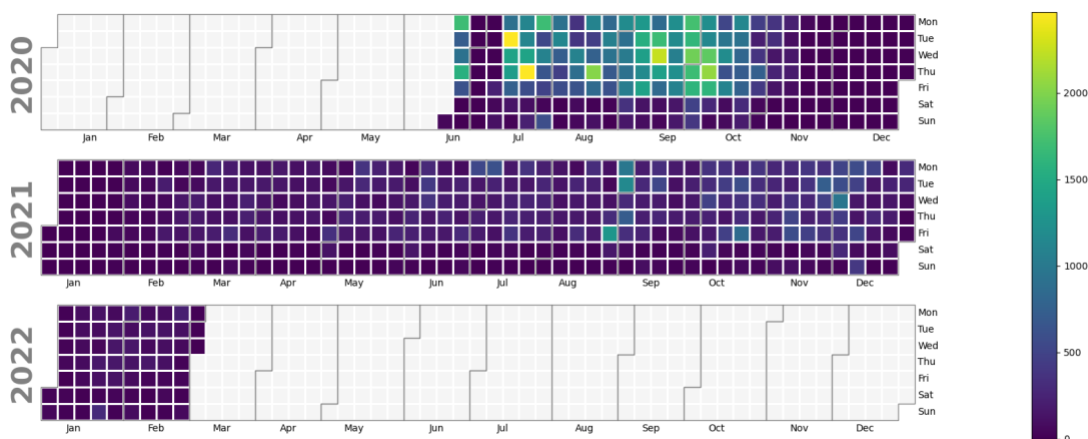


Figure 1 - Heatmap of leaked conversations, shows the number of messages per day

Below, we present some of the points we found more useful to share because of the insights they provide on how a ransomware group operates.

## 4.1. Organizational Chart

Table 2 shows a list of aliases of the Conti members that had the most interesting conversations. As the leaked chats contain a huge amount of information, we would like to stress that this information is incomplete. Overall, as observed by other [researchers](#), the overall structure is quite similar to a modern startup company, with several decentralized teams working on various different projects. Some of the members have a strict role (e.g., HR, developer, or a ransom negotiator).

**Table 2 – List of identified Conti members and their roles**

Alias	Role
<i>stern</i>	Boss 1
<i>tramp</i>	Boss 2
<i>hof</i>	sysadmin, oversees botnets
<i>zevs</i>	sysadmin, oversees botnets
<i>max</i>	Alla Witte, the Trickbot developer
<i>revers</i>	Hacker, manager
<i>professor</i>	Negotiates ransom with companies, creates darknet blogs
<i>Hors</i>	Sysadmin
<i>Bentley</i>	Sysadmin
<i>Swift</i>	hacker
<i>Buza</i>	Developers' teamlead / OSINT research
<i>pumba</i>	Negotiates ransom with companies, creates darknet blogs
<i>bio</i>	Negotiates ransom with companies, creates darknet blogs
<i>skippy</i>	HR / Legal
<i>many</i>	works on cryptolocker, decrypts data for victims
<i>starfall</i>	Sysadmin
<i>reshaev</i>	top hacker
<i>Salamandra</i>	HR
<i>kagas</i>	HR
<i>viper</i>	HR
<i>elvira</i>	HR

<i>ford</i>	HR
<i>jaime</i>	Developer
<i>mango</i>	technical manager, QA, side projects (blockchain, hackers' social network)
<i>cybergangster</i>	works on cryptolocker, decrypts data for victims
<i>dollar</i>	Hacker, works as intermediary between the group and the victims
<i>pin</i>	works on cryptolocker, decrypts data for victims
<i>paranoik</i>	works on cryptolocker, decrypts data for victims

## 4.2. Exploits, in-house tools, and social engineering

There are several discussions about exploit development, use of in-house tools, and social engineering:

- Discussions about buying **Sonicwall** and **Cisco** routers/firewalls for vulnerability research and exploit development (most likely, **CVE-2020-5135**). There is a request from *stern* sent to many members at once, asking if anyone can write a custom vulnerability scanner for a Sonicwall device.
- According to some discussions, Conti team members may buy 0-day exploits from third-parties.
- Conti team members relied on social engineering tactics quite heavily. There is evidence that they “bluff” by telling hacked companies they have their data and are ready to publish it, while they don’t have anything. As mentioned before, they use lawyers to understand how victims can be intimidated into paying the ransom. Also, it seems that Conti members heavily rely on spam/phishing campaigns, and use specialized software to carry them out.
- The group constantly works on anti-virus evasion: each new build is being tested against modern AV solutions. Also, they managed to purchase a license for **VMWare Carbon Black** for their tests, which took them quite a bit of effort and 3 months of time.

## 4.3. Conti Victims

- There are several Healthcare targets mentioned in the chat, and several hospitals mentioned on the Conti leaks website. This is a bit controversial, since some members discuss that they “**agreed on the fact that healthcare targets are off limits**” and there was one person mentioned in the chat (**dollar**) who they want to expel from the group for breaking this rule.
- Below, we present some charts about companies mentioned in the chats, giving insights on how many have paid the ransom and how many have not.
- We identified 84 organizations mentioned in the chats for which there is limited public information of them being attacked.
- From our analysis (Figure 2) emerges how the Conti group targets companies of any size in almost equal parts.
- US companies are by far the ones more targeted (49 out of 84 in our sample) followed by Germany and Canada as shown in Figure 4

- Services and Manufacturing represents the sectors mostly impacted by Contis' attacks.

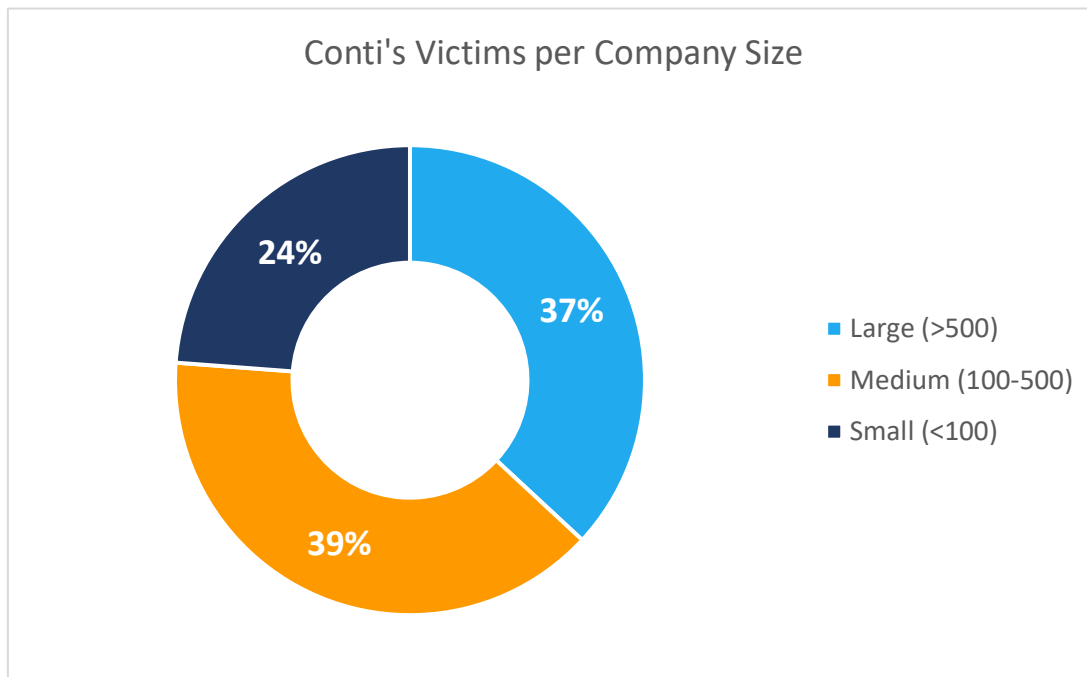


Figure 2: This chart shows how the Conti's group targets all kind of organizations independently from their size (measured as number of employees)

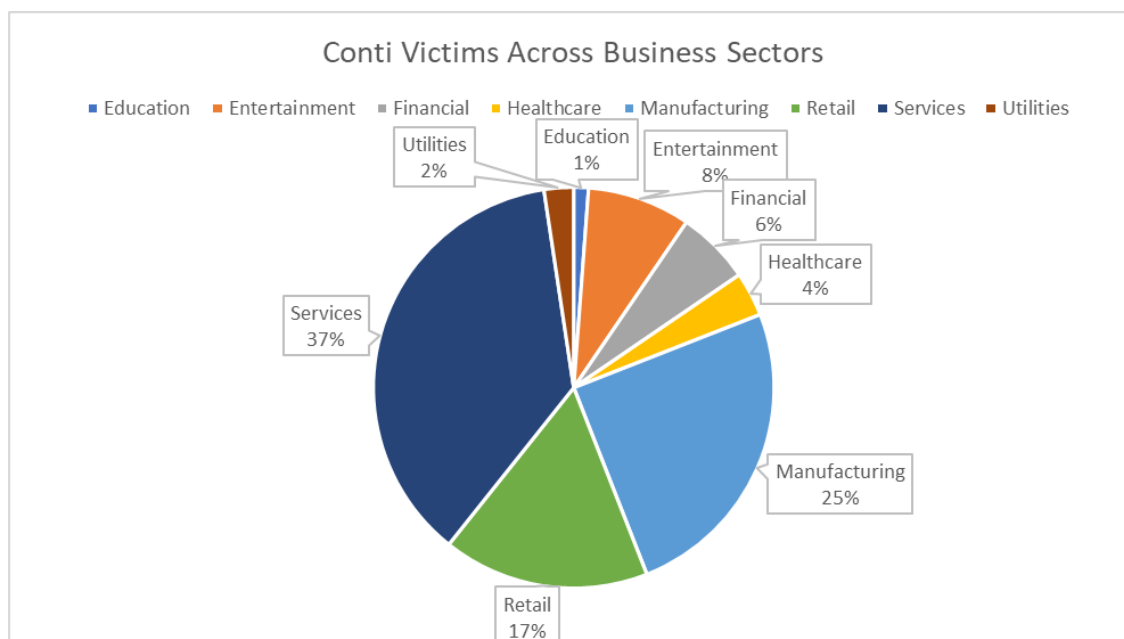


Figure 3: This chart shows how Conti's victims mostly fall under Services and Manufacturing



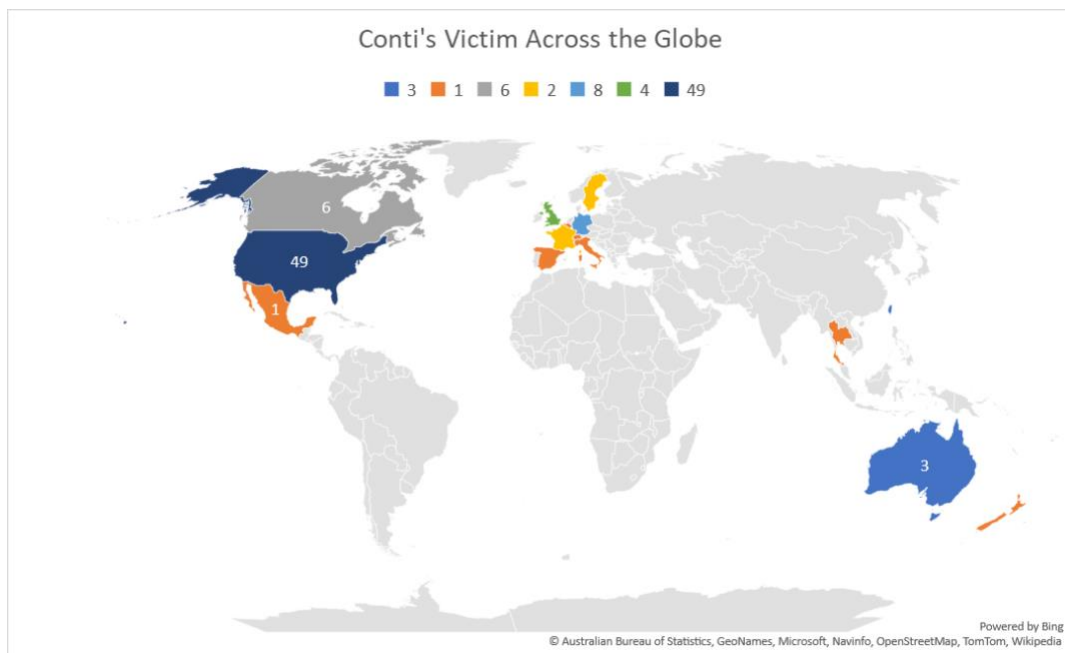


Figure 4: This chart shows the Countries the Conti's group targeted more often

#### 4.4. Tidbits

- There is evidence that the members of the group negotiate with access brokers.
- There was a discussion about “leasing” Trickbot to other hacking groups for half the profits.
- There is a mention to the **Diavol** ransomware that was not previously attributed to the group. *stern* is very angry about some developers that reused parts of **Trickbot** for this new ransomware – and it gave them away (he refers to a Russian version of a [publication about this](#)).
- They discuss that someone has an inside person in several Indian banks (e.g., **Axis Bank** is mentioned) and one bank in Kosovo. It’s unclear whether they wish to use this contact for hacking or money laundering.
- There are some discussions that reveal the political stance of some of the members:
  - *mango* and *professor* discuss they got access to emails of someone from Bellingcat who “works against Russia”. They are discussing publishing this data because they are “patriots”. It seems, there are some files concerning the Alexei Navalni investigation by FSB among the leak.
  - Many members really enjoy the fact that the Russian invasion into Ukraine has started.
- We found evidence that the members of the group were seeking legal help for various things, such as:
  - Some members (e.g., *skippy*) had connections with lawyers to understand whether a victim can be successfully extorted based on the local customer data protection laws.
  - *mango* and *stern* discussed hiring a lawyer for Allaa Witte (*max*), [a Latvian national convicted for Trickbot](#), who has been a member of the group;
  - On 3<sup>rd</sup> of November 2021, *kagas* tells *stern* that “their old case has been re-opened” by the Russian police. They have done it following the request of the US police. In particular, they were interested in people related to Trickbot. *kagas* mentions that they are in contact with their lawyers, and they should “lay low” until 13<sup>th</sup> of November 2021.

- We found evidence that Conti has been planning to launch a couple of side projects in DarkNet: a cryptocurrency stock exchange, and a social network where blackhats can connect and share knowledge (*mango* and *stern* have been involved into these discussions, but the original idea belongs to *stern*).

## 5. Analysis of Tutorials and Documents

Out of the leaked documents, we focused our analysis on two that are relevant to understand Conti's attack techniques: the "hacker's quickstart guide" (Section 5.1) and the "researcher's quickstart guide" (Section 5.2).

### 5.1. Hacker's quickstart guide

One of the leaked Conti documents contains a file called "*быстрый старт хакера.txt*" which can be translated as "*hacker's quickstart guide*". The file contains general recommendations for attacking computer networks and gaining persistence. This file outlines general techniques and recommendation for penetrating computer networks. The main points of interest can be summarized as follows:

- **IoT devices are a major initial attack surface.**
- **RDP is recommended as an "initial backdoor."**
- **Active Directory / Domain Controllers are often the primary target before achieving persistence.**

Below we provide some takeaways from translating the document.

#### Choosing a point of entry

Any public network service (e.g., public IP address with an open port) is a potential point of entry. If an attacker can't easily get through via a known vulnerability, they should pivot. There are several other plausible vectors:

- Specialized hardware (IoT/OT) such as printers, routers, smart firewalls, PLCs (**NOTE: this correlates with some evidence from the chats that the group was actively looking to purchase Cisco and SonicWall routers for exploit development**);
- Popular web applications such as WordPress or other Content Management Systems;
- Botnet entry points (e.g., dormant infections within IT/IoT equipment).

In particular, IoT/OT targets are not being updated often due to various reasons: (1) some updates may disrupt the functioning of critical processes; (2) vendors often do not offer support after N years, so the updates are not possible (it also happens with relatively new hardware). Moreover, the author of the document expresses a feeling that specialized hardware targets, such as IoT and OT devices, are not being treaded seriously within the cybersecurity field.

#### Legitimate services such as VPN and RDP help to achieve an "ideal backdoor"

Legitimate services such as VPN, thin clients, RDWeb, and RDP which are exposed to public networks can help in creating an "ideal backdoor". These services can be used to hide any malicious traffic and ensure that attackers remain unnoticed.

Therefore, attackers should look for any credentials and computers available within the target network that can be used to access these services. Often, weak passwords are used for them, and it is quite common that the same credentials are used for multiple services/machines within the same network.

If leveraging such services fails, attackers can try to hide their traffic via common business software such as Microsoft Outlook, IIS/PHP webshells and similar. Finally, network protocols like DNS, TCP, and HTTPS can be used for this purpose. Using common Windows services can also be an option, but it is discouraged because standard OS functionality can be closely monitored by anti-virus software.

### *Windows Active Directory / Domain Controllers is the primary target*

The primary goal of most attacks is Active Directory / Domain Controllers within Windows-based networks. Access to such network nodes allows, at the very least, for wide lateral movement capabilities. At most, it allows for getting full control over the target network(s). Active Directory servers are most convenient for exploitation: often, typical misconfigurations can be found, there are plenty of vulnerabilities (such as [ZeroLogon](#)) and common resources enabled by default (e.g., default network shares). In particular, such common resources not only help regular employees to do their day-to-day job, but also make the job of the attackers significantly easier.

### *Typical frameworks that should be used*

Nowadays, the common hackers' tools revolve around various open-source frameworks. Using these frameworks can help to quickly automate various routine tasks. In particular, the following ones are mentioned:

- *Metasploit Framework* (MSF) – one of the largest collection of exploits and modules.
- *Core impact* (+*Impacket* written in python) – offers the most convenient features for penetration testing. Works only for Windows environments.
- *Powershell Empire* – pure powershell framework “with all the bells and whistles” for penetration testing and exploitation.
- *Posh2c* and *Koadic* – C&C (Command and Control) frameworks used for post-exploitation and lateral movement. The traffic that these frameworks produce is hard to detect.
- *Cobalt Strike* – an adversary simulation tools that can emulate various TTPs of threat actors. While this framework is intended for simulating attacks, it is quite often used by attackers. The framework allows for great extensibility.
- *Burp Suite* – a good framework for web application penetration testing.
- *Puppy* – a Remote Administration Tool (RAT) written in Python. It works well against anti-virus software, since it produces artifacts in its native code that is difficult to analyze.

Still, the main downside of all public tools is the fact that they are well-known for anti-virus software. One must make great efforts to obfuscate them, therefore it may be often better to make bespoke tools.

### *Social engineering is important*

If everything else fails, social engineering is the last resort. An email or a phone call can achieve great results. Some other tutorials contain instructions on how useful information can be collected from social platforms such as [LinkedIn](#).

## 5.2. Researcher's quickstart guide

Another tutorial of interest is called “быстрый старт исследователя.txt” which can be translated as “researcher's quickstart guide.txt”. The document is quite extensive and contains a lot of technical information about topics around program obfuscation techniques, process injection and anti-virus evasion.

We do not provide a translation of this guide because it would significantly increase the length of this report. The main topics discussed are:

- Various tools and techniques for process injection.
- Defensive techniques used by anti-virus and intrusion detection tools and ways of circumventing them.

- Anti-debugging and anti-sandbox techniques that should be employed by the malware to thwart analysis, should the malware sample be acquired by third parties.
- Persistence, privilege escalation, and C&C tools and techniques.
- Code hardening and optimization techniques, cryptography.
- Typical living-off-the land attacks (LOLBAS) that can be performed once the target network has been penetrated.

There are some interesting notes that mention “network asymmetry”. These notes can serve as a consideration for targeting businesses and agencies within the geography of the so-called “collective West”. It translates as follows:

*The effectiveness of an anti-virus (AV) solution depends on the country. Most of the AV software vendors are from the Western countries. The effectiveness of the AV software depends on various checks that are implemented using neural networks, these checks are typically executed somewhere in cloud environments. With the beginning of cyber-confrontation between the US and Russia, the US has prioritized the AV traffic analysis destined to their country, to the detriment of the analysis of the traffic bound to other countries (including the countries of Western Europe). The US did it to increase their own security posture. It seems like they don't have unlimited resources, after all. Therefore, it's quite common when the same "payload" doesn't work in the US, but it works for any other country.*

## 6. Analysis of Tools

The source code of three main collections of tools have been leaked: first, a version of the TrickBot malware; second, a set of internal tools used for purposes such as affiliate management and victim data collection; third, the locker and decryption components. In the sections below, we briefly discuss each of these collections.

### 6.1. TrickBot

The leaked TrickBot source code contains two components: “dero” (a command dispatcher) and “lero” (a data collector) built using Erlang. Conti uses these components to deploy a C&C server to collect data from and dispatch commands to their victims. Victim data sent to the server via HTTP POST requests includes *Time*, *Client ID*, a *Group tag*, a list of processes and system information. This collected information is stored in a Postgres SQL database.

### 6.2. Internal Tools

The leaked internal tools are described in Table 3.

**Table 3 - List of internal Conti tools**

Component	Description
Chimaera.Ngrok	Tool from <a href="#">TeamTNT</a> used to expose compromised internal machines to the internet
Chimaera.Sugarlogic	Another tool from TeamTNT. Uses <i>xmrig</i> to mine Monero.

admin	A web application built on Kohana as an admin panel.
backdoor.js.git	A git repository hosted on <a href="https://vya52lgt7p65rxz.onion/steller/backdoor.js">https://vya52lgt7p65rxz.onion/steller/backdoor.js</a> . There is a Perl script using <i>watchman</i> ( <a href="https://facebook.github.io/watchman/">https://facebook.github.io/watchman/</a> ) to monitor file activities on victim machines.
backdoor-master	Botnet targeting Windows victims and supporting the following commands: Sleep, Get info, Run EXE, Run DLL, Run BAT, Run PowerShell, Reset, Terminate Process, Download File, Run Code, Suicide, Update loader x86, Update loader x64, Update bot x86, Update bot x64
cadmin-master	Web application that serves as an admin panel to manage users and view their activities Uses <i>Kohana</i> and <i>Postgres</i> for managing databases that include User ID, User IP, Session ID, User Agent
import-master	Collects the following information from the victims: Credentials, OpenSSH private keys, OpenVPN passwords and configs, OWA passwords, IE passwords, chrome passwords, Edge passwords, firefox passwords, Outlook passwords, FileZilla passwords, WinSCP passwords, PuTTY passwords, VNC passwords, RDP passwords, TV passwords, git passwords, KeePass passwords, AnyConnect, bitcoin, Litecoin.
sendmail-master	A web application based on Laravel to exchange emails.
spoked-master	A web application based on Laravel.
srw-master	A web application based on Laravel.
storage_ebay_checker-master	A PHP script to check the balance of a user on Ebay.
storage_ex-master	A Kohana-based web framework for managing databases (seems to be deprecated).
storage_go-master	A Go module to parse, store, and query IP addresses.
storage-master	A Kohana-based web framework for managing databases (seems to be the active one)

### 6.3. Locker

Table 4 describes the locker components. Both the locker and decryptor use the *chacha* library (encrypted key: 524 bytes, chacha key: 32 bytes and chachaIV: 8 bytes). There are four encryption targets (local, network via SMB port 445, backups, and full) and two encryption modes (header, partial and full). The locker maintains a list of blacklisted directories (e.g., *Boot*, *Trend Micro*) and files (e.g., *.exe*, *.msi*), chooses the encryption mode based on file extensions, uses a mutex to prevent infecting the same files, renames encrypted files with the extension *.EXTEN* and store logs at *C:\CONTI\_LOG.txt*. The locker uses anti-hooking techniques to evade detections.

One interesting point that stood out in the analysis is that the name of one of the locker/decryptor author is probably *Anton* because there is a commented out path used for testing that contains the username “toha”, which is a common nickname for Anton.

**Table 4 – List of Locker components**

Component	Description
builder	Conti built the malware using Visual Studio .NET. The malware targets Windows users of both x86 and x64 architectures.
decryptor	This module provides functionalities to decrypt files encrypted by <i>locker</i> .
locker	This module contains main functionalities such as network scanner and encryption.
Release	There are two executables: <i>locker.exe</i> and <i>decryptor.exe</i> .
x64	This is supposed to contain the binaries generated for Windows x64.

## 6.4. IoCs

Based on the analysis of the tools above, we mention some identified IoCs:

IoC	Description
F2F57926-ED6C-4052-B9B5-D7B45F98F562	ProjectGuid of <i>locker</i>
A9D7F611-98C5-496E-AD28-5C92ADD2A8E2	ProjectGuid of <i>decryptor</i>
kjsidugidf99439	Mutex used by <i>locker</i>
97b1b747e07b45e5166eeaaf6b2fbcfc0cfc5f92bcfef8f1e9be38cdc72d1c8e	<i>locker.ex_</i>
1dca7a9ea1b94aa5b1052f79f79ea65fcc950f9f1b24d7e09f9281886dbc72b5	<i>decryptor.ex_</i>
megahoster.dedicatedpanel[.]com	Domain hosting the admin panel
188.138.1.53	IP address used by <i>lero</i> , <i>sendmail</i>
185.25.50.238	IP address used by <i>srw-master</i>
179.43.147.243	IP address hosting the backdoor.js
45.142.215.227	IP address mentioned on the C&C

© 2022 Forescout Technologies, Inc. All rights reserved. Forescout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents is available at [www.forescout.com/company/legal/intellectual-property-patents-trademarks](https://www.forescout.com/company/legal/intellectual-property-patents-trademarks). Other brands, products or service names may be trademarks or service marks of their respective owners.