


# Conti Affiliate Exposed: New Domain Names, IP Addresses and Email Addresses Uncovered

 [esentire.com/blog/conti-affiliate-exposed-new-domain-names-ip-addresses-and-email-addresses-uncovered-by-esentire](https://esentire.com/blog/conti-affiliate-exposed-new-domain-names-ip-addresses-and-email-addresses-uncovered-by-esentire)

BLOG

## Conti Affiliate Exposed: New Domain Names, IP Addresses and Email Addresses Uncovered by eSentire

**eSENTIRE**

A Cobalt Strike Cybercrime Syndicate and the Ransomware Hackers' Favorite Weapon

On March 9, the Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Secret Service issued an updated [alert](#) about the Conti ransomware group, encouraging organizations to review their advisory and apply the recommended mitigations. They stated: “Conti cyberthreat actors remain active and Conti ransomware attacks against U.S. and international organizations have risen to more than 1,000. Notable attack vectors include Trickbot and Cobalt Strike.”

eSentire’s Threat Response Unit security research team (TRU) has been tracking the movements of the Conti gang for over two years. TRU [issued a new report](#) on the [Conti Gang](#) on March 7, 2022, two days prior to the CISA alert, where it warned its customers and critical infrastructure organizations that the Conti gang was continuing to launch attacks against oil terminals, pharmaceutical companies, food manufacturers, IT services providers, etc. Conti declared its allegiance to Russia immediately following Russia’s invasion into Ukraine.

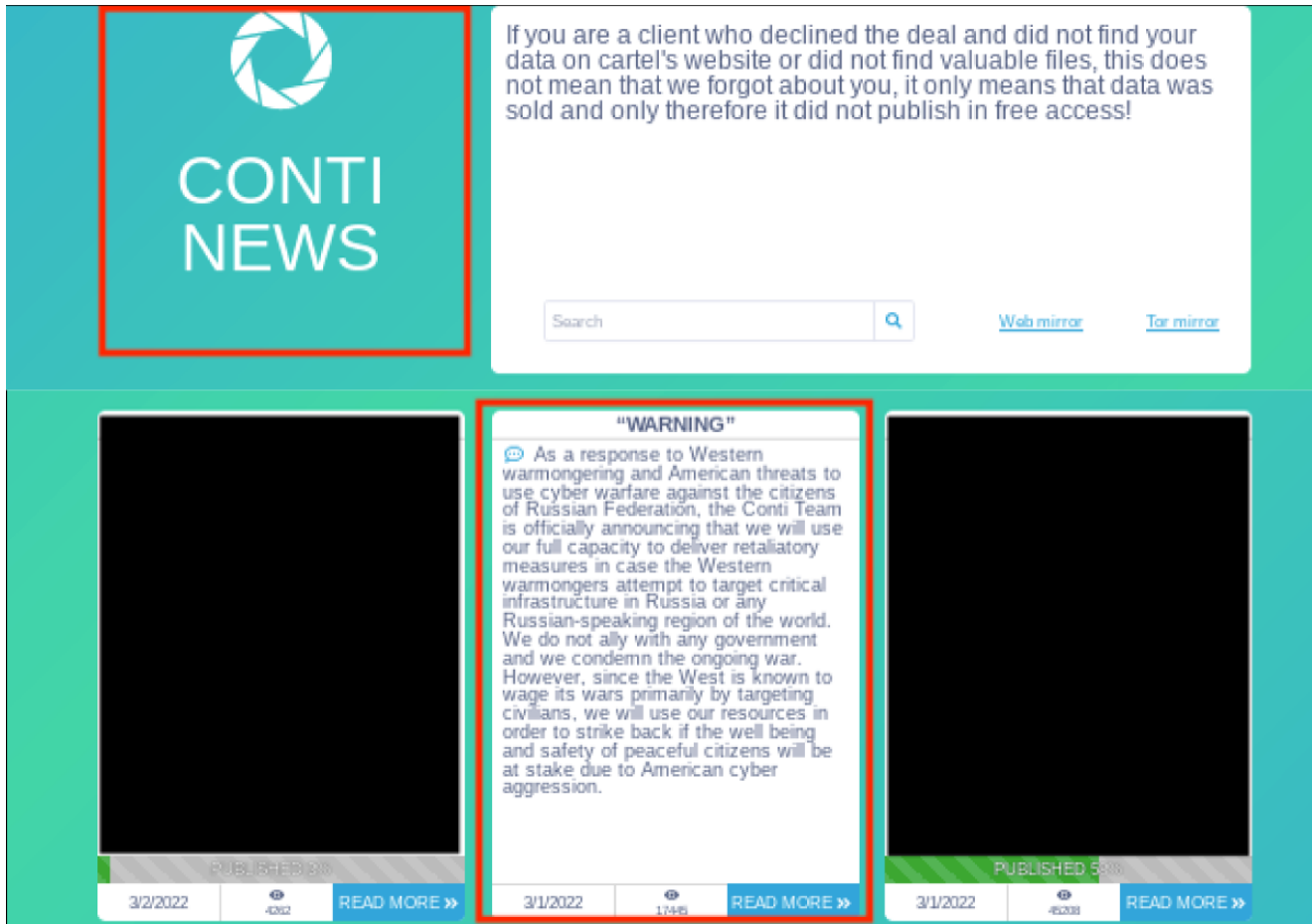


Figure 1: Conti's Name and Shame Site indicating allegiance to Russia.

TRU is publishing a new set of Indicators of Compromise (IOCs), which are currently being used by a Conti affiliate, and eSentire is encouraging security defenders to also use these to detect any possible Conti activity in their networks. These IOCs all link back to the Cobalt Strike infrastructure.

Every week for the past three years, the public has heard countless news reports of businesses and public entities being compromised by ransomware. However, in these incidents, it is usually the ransomware groups behind the attacks that grab the headlines. TRU contends that it is not just the ransomware gangs that are causing the scourge, it is also those cybercriminals who are supplying the malware, the infrastructure and the tools. For some time, what appears to be their favorite weapon is Cobalt Strike. Cobalt Strike has repeatedly enabled ransomware threat actors to disrupt critical healthcare services, municipalities, educational institutions, energy companies, and international meat suppliers.

For the past year and half, Cobalt Strike (a threat emulation software used for adversary simulations and Red Teams) has been observed being used by the top ransomware gangs and financial cybercrime groups. Cobalt Strike is an organized, methodical and multi-functional software that is being used, unfortunately, in conjunction with ransomware to disrupt critical systems. It is readily delivered by numerous initial access vectors and provides a variety of tools that help threat actors navigate around defenses.

## Burning a Conti Affiliate's Cobalt Strike Infrastructure

---

TRU has been tracking the operations of an active Conti ransomware affiliate since August 2021. During TRU's research, it discovered that cybersecurity company [BreakPoint Labs \(BPL\)](#) had also been studying the same Conti affiliate. Therefore, eSentire and BreakPoint Labs began sharing their findings with one another and uncovered some important details relating to this affiliate, its infrastructure management methods, and its use of Cobalt Strike. It is also important to note that the main [Conti operators have recently brought the Trickbot](#) authors, Wizard Spider, into their operation. Members of the Trickbot gang are long time partners of Conti, and they have recently developed BazarLoader which downloads additional malware onto a victim's computer.

Interestingly, TRU observed this affiliate's Cobalt Strike infrastructure being leveraged in two subsequent ransomware attempts on Valentine's Day of 2022, just as the tensions between Russia and Ukraine were escalating.

The speed and efficacy of both the intrusion actions and the infrastructure management indicate automated, at-scale deployment of customized Cobalt Strike configurations and its associated initial access vectors. Customization choices include legitimate certificates, non-standard CS ports, and malleable Command and Control (C2). In this report, we will examine associated ransomware operations, including operations that rely on:

- SonicWall exploits
- Shathak (TA551) and TR (TA577) malware distribution operations
- BazarLoader and IcedID malware
- The Cobalt Strike intrusion framework
- FiveHands/HelloKitty/DeathKitty ransomware and Conti ransomware

TRU observed sophisticated intrusions conducted from the infrastructure, which are detailed below, followed by an exploration of the features of the infrastructure. Finally, a list of indicators comprising the vast Cobalt Strike deployment are provided.

## Cobalt Strike at Scale

---

Following a series of leaks of the Cobalt Strike Intrusion Suite starting in 2020, the tool quickly rose to prominence in ransomware intrusions. Throughout 2021, eSentire's TRU observed that – with few exceptions – hands-on- intrusions invariably relied on Cobalt Strike (Figure 2). The trend continues into 2022 alongside [yet another](#) leak of Cobalt Strike's latest version. With each successive leak of the tool, threat actors gain additional features that help them to evade security and manage [intrusions at scale](#).

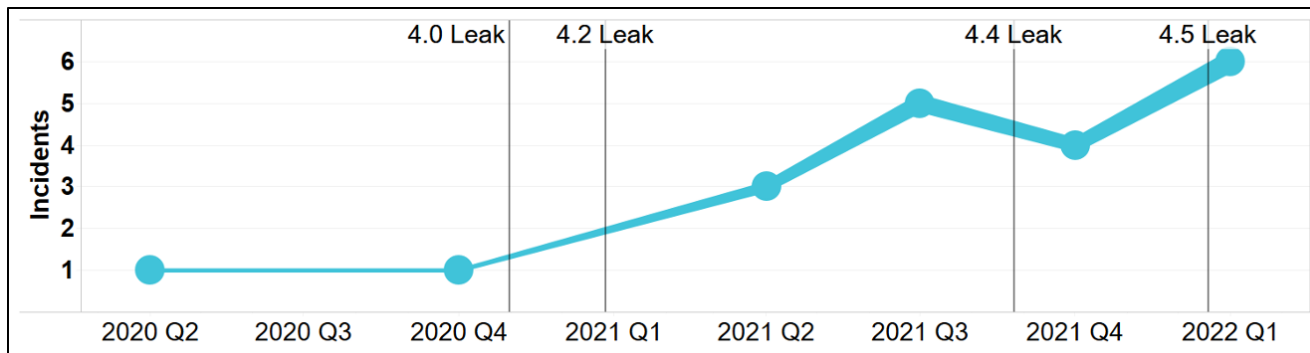


Figure 2: Cobalt Strike observed by TRU in incidents (blue trace) and timing of Cobalt Strike source code leaks to the public (vertical black lines)

## Why has Cobalt Strike become so popular for ransomware campaigns?

Ransomware intrusions are full-scale organizational intrusions that require actions such as discovery, lateral tool transfer and privilege escalation (Figure 3). Not only can Cobalt Strike do all of that, it can also change up its disguises using malleable C2 and an artifact kit to evade network and endpoint security. Threat actors need only deliver Cobalt Strike’s Beacon – a highly configurable backdoor that allows attackers to quietly and remotely control endpoints and inject other attacker tools – as a payload of their chosen initial access vector, and Beacon will point back to an attacker – controlled Team Server, where attackers can log on and intrusions can be orchestrated. Due to Cobalt Strike’s relative simplicity, it enables lower-tiered threat actors to act in supporting roles to ransomware operations, allowing for ransomware gangs to scale out their operations and increase efficiencies.

In short, the tool puts most of the features you’d find in other malware in one place. MITRE describes the tool as follows: “Cobalt Strike’s interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.” Cobalt Strike has been in use and continuously updated with new functionality for at least the past ten years. It is an “adversarial simulation software,” the developers (have continuously added evasive features, observed in the wild, to its pen testing capabilities). Cobalt Strike also has a public community that openly shares aggressor scripts, which allow various plugins and integrations to be written for Cobalt Strike, and Beacon profiles, which define various communication protocols for C2. Thus, for many backdoors and RATs available on the underground market, Cobalt Strike is capable of the same functionality, plus more.

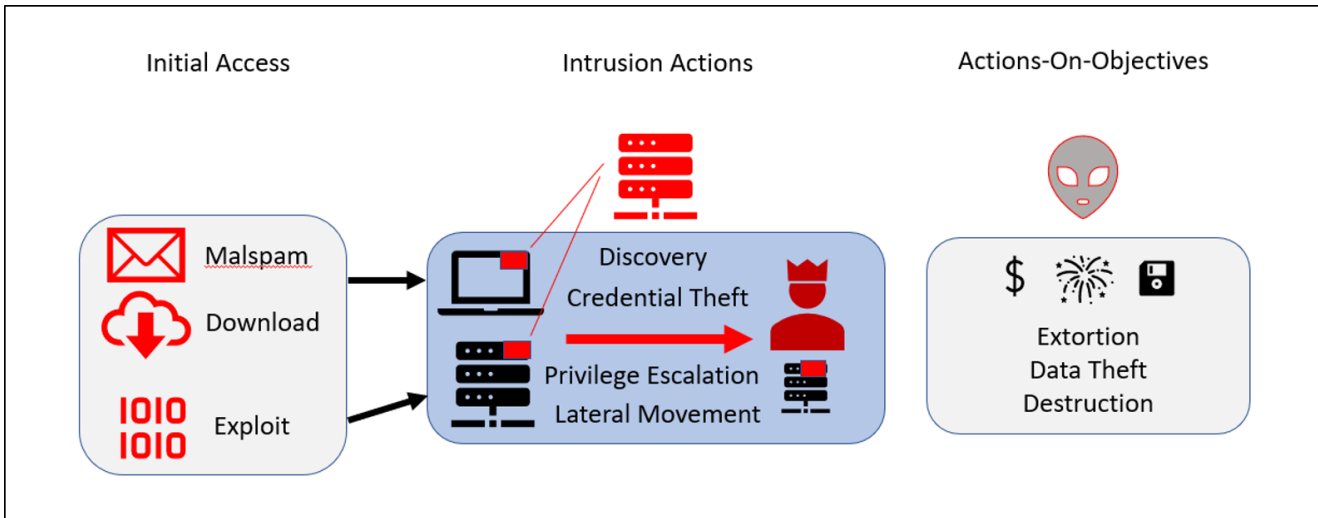


Figure 3: In the simplified kill chain model, Cobalt Strike can directly perform most intrusion actions allowing the operation to efficiently achieve their objectives

## Ransomware Operations Utilizing the Cobalt Strike Infrastructure

TRU observed at least two cybercrime operations utilizing the same Cobalt Strike infrastructure, during 2021 and into 2022, and both operations are leveraging SonicWall exploits to deploy a Go variant of the FiveHands/HelloKitty/DeathKitty ransomware family and they are also employing initial access brokers, associated with the Conti Ransomware operation. Earlier in the year, SonicWall exploits being used in FiveHands ransomware campaigns (Figure 4), were associated with FiveHands affiliate UNC2447. A 2021 report by Mandiant notes the group had previously deployed RagnarLocker. Symantec has since associated UNC2447 with recent campaigns deploying Yanluowang Ransomware.

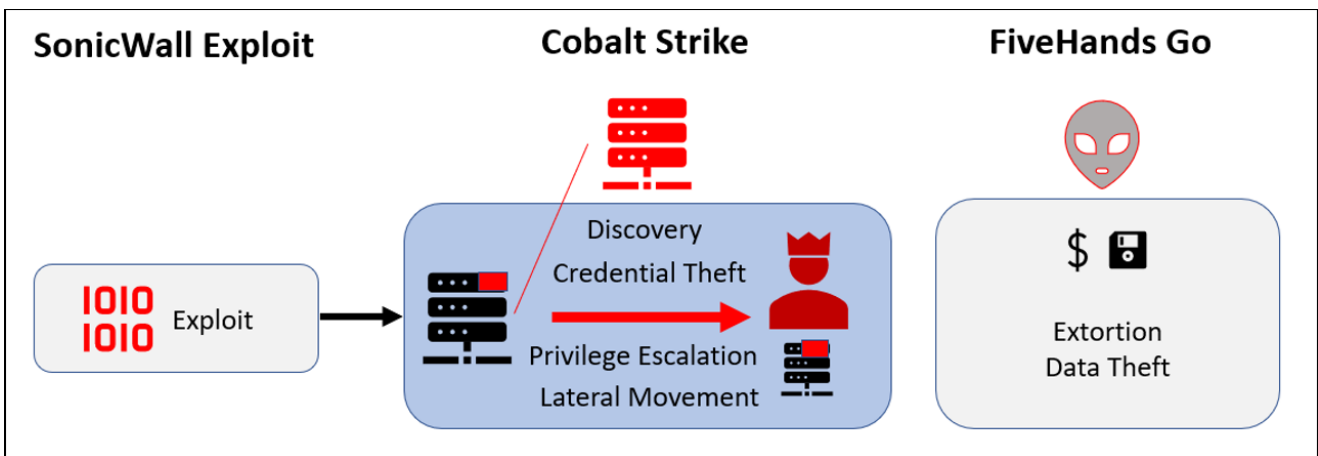


Figure 4: A campaign utilizing SonicWall exploits leveraged the tracked Cobalt Strike infrastructure to deliver a Golang variant of the FiveHands Ransomware

More recently, the same Cobalt Strike infrastructure was observed being leveraged in Conti ransomware deployments via Shathak (aka TA551) for initial access (Figure 5). Shathak is a threat group known for launching phishing campaigns that typically utilize malicious documents, and these often lead to backdoors, such as IcedID. TRU has seen some overlap

in these campaigns with the TR botnet (aka TA577), which delivers payloads via malicious documents and which tends to use the same toolset as the Shathak malicious phishing campaigns.

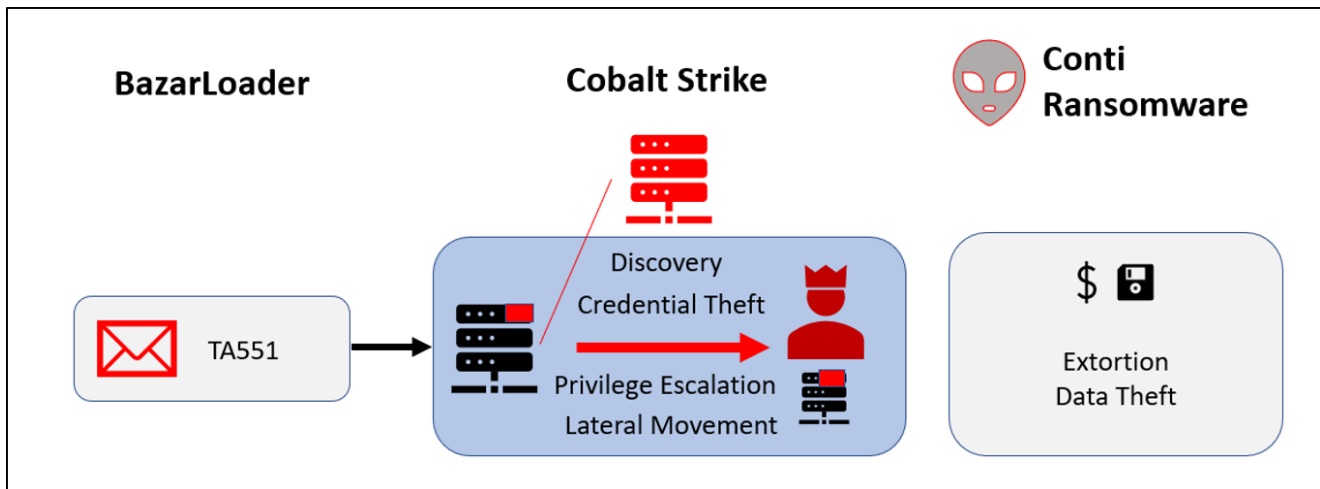


Figure 5: An operation by the Shathak Group (aka TA551) leveraged BazarLoader through malicious emails. BazarLoader allowed the operation to pivot to the tracked Cobalt Strike infrastructure for Conti deployment.

## Syndicate Infrastructure

Management of the Cobalt Strike infrastructure appears to be highly automated, potentially relying on automated name server generation via reseller API. Legitimate and trusted certificates are deployed to the infrastructure within minutes of domain name creation. Domain names used for Cobalt Strike Command and Control (C2) reflect a common naming scheme, typically two to three words or acronyms that reflect common information technology and known brands. The infrastructure rotates through a consistent range of open ports and registrar choices (Figure 6). TRU's analysis of the Conti chat leaks provides some insight on infrastructure management within the Conti team, but it's not clear how entwined the domains tracked here are with this core Conti group. However, the primary candidates from the leaked chats would be Carter's infrastructure through which Bentley's builds integrate the different tools and malware involved (such as BazarLoader, Cobalt Strike and the ransomware itself). An excerpt of the domain names, IP addresses and email addresses being used by this Conti affiliate are enclosed below. It appears that this Cobalt Strike infrastructure management group has also relied on a variety of ProtonMail email addresses to register some of their domains:

[email protected]  
[email protected]  
[email protected]  
[email protected]  
[email protected]  
[email protected]

[email protected]

[email protected]

[email protected]

[email protected]

## **Excerpt of the Cobalt Strike C2 Domain Names and IP Addresses Utilized by a Conti Affiliate**

---

firmwareupdater[.]com  
aspdotnetpro[.]com  
fortinetdirect[.]com  
intergroupservices[.]com  
thumbsupdating[.]com  
estudiopay[.]com  
appnewrelease[.]com  
gpupdatemanager[.]com  
flashpointdatabase[.]com  
wirelesswebaccess[.]com  
webdatabasesystem[.]com  
46[.]21[.]153[.]52  
23[.]227[.]196[.]236  
146[.]70[.]44[.]201  
198[.]252[.]99[.]99  
172[.]96[.]186[.]51  
23[.]227[.]202[.]142  
23[.]227[.]198[.]235  
46[.]21[.]153[.]48  
23[.]227[.]198[.]211  
23[.]227[.]196[.]58

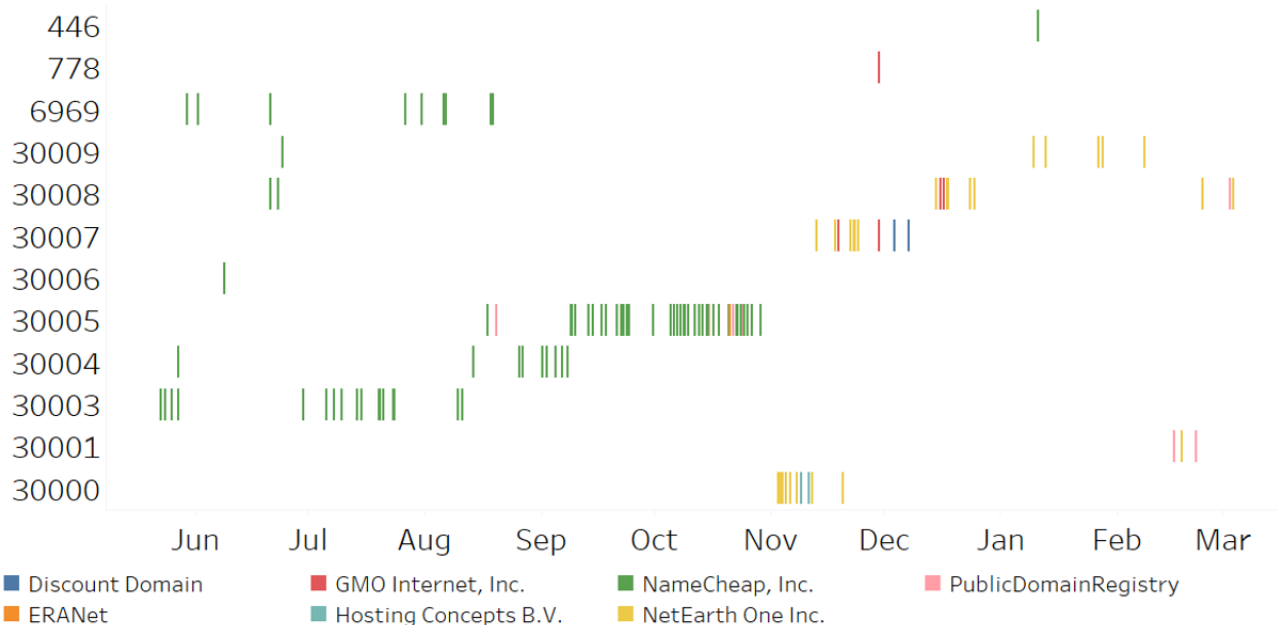


Figure 6: Ports and Registrars observed at time of domain creation

## Sophisticated Intrusions

Combined, TRU and BPL observed the Cobalt Strike infrastructure being leveraged to attack seven different U.S. companies between 2021 and 2022. The victims include companies in the financial, environmental, legal and charitable sectors.

In July 2021, the threat actors behind the Cobalt Strike operation compromised four different financial organizations via one technology provider, which each of the victims were using to manage their IT environments. Since the technology provider deployed SonicWall as a VPN solution for its customers, the financial organizations were rendered vulnerable to the previously mentioned exploits. In these cases, the threat actors were able to delete cloud-stored backups prior to ransomware deployment. Luckily, the financial companies had other, more recent backups, to restore from – a good lesson to follow. The ransomware was later determined to be the late Go Version of Feral Spider and shared similarities to previous FiveHands and HelloKitty variants.

More recently, on Valentine’s Day 2022, amidst escalating tensions between Russia and Ukraine, the TRU intercepted an attack leveraging the Cobalt Strike infrastructure in which the threat actors were trying to breach a children’s charity and, hours later, they attempted to breach a legal firm. However, one attack stands out as a demonstration of the power and capability of the Cobalt Strike Intrusion Suite, should it land in the wrong hands: the **ShadowBeacon** Incident.

## The Cobalt Strike ShadowBeacon Incident



The TRU observed the first Cobalt Strike Beacon early in the morning during the summer of 2021. The Beacon instance presented an immediate mystery – it pointed to an internal device. The infected host was isolated and an investigation into the source of the signal was opened; another Beacon appeared. Again, a host was isolated. The Beacons were being deployed from the domain controllers via PsExec, a legitimate administrator tool used for remotely executing binaries. This time; however, the internal IP was different. Sensing an active hands-on intrusion, TRU began manually deleting the Beacon instances just as eSentire’s incident handlers were finding an answer to the shifting Command and Control channel. The intruders were using Forty North’s C2Concealer. The Beacons were SMB Beacons, which utilize the organization’s internal SMB traffic for its C2. That meant that the cloaked internal device likely had an HTTP Beacon–through which it was funneling the traffic from SMB Beacons to the exterior Cobalt Strike C2 Server. The more common Beacon utilizes standard internet protocols.

To gain further intelligence around the mysterious internal device required a review of the Windows logs. Given that the customer wasn’t ingesting their log signals into eSentire’s Atlas XDR platform, a manual request for logs was initiated, introducing a delay to the investigation. With domain control and a cloaked machine, the attacker continued to deploy SMB beacons, struggling to maintain a foothold as incident handlers continued to shut down Beacon instances. But after receiving and manually reviewing the Windows logs, TRU discovered the intersection of the SMB traffic and patient zero.

## **Crafty Threat Actors Bring Their Own Virtual Machine**

---

The Windows logs revealed that the threat actor had been able to register their own virtual machine on the victim organization’s network, using it as a pivot to their actual, exterior C2. With the source of the infection no longer hiding in the VPN pool, the attacker was kicked out and the recovery process started. No ransomware was observed.

## **Cobalt Strike Infrastructure-Campaign Links**

---

### **Conti Playbook and Intrusion Tools Used in the ShadowBeacon Incident**

---

The recent leak of a Conti message board provides a thorough set of tools and practices used by Conti. The following was observed in both the ShadowBeacon Incident and Conti’s expansive playbooks:

- SonicWall Exploits
- Forty North’s C2Concealer
- Bring Your Own Virtual Machine (BYOVM)
- The use of VPS servers for C2

## **SonicWall Exploits and FiveHands Ransomware**

---

June 2021 – CrowdStrike [reports a new variant](#) of Go ransomware

August 2021 – BreakPoint Labs [reports numerous domains](#) associated with the previously mentioned breaches. The hashes reported by CrowdStrike, and BreakPoint Labs share [vhash similarity](#) in VirusTotal

August 2021 – eSentire observes the Cobalt Strike ShadowBeacon Incident.

## **Shathak, BazarLoader, IcedID and Conti Ransomware**

---

August 2021 – **amibios-updater[.]com** is [reported by Brad Duncan](#) of Palo Alto Networks' Unit42 in association with TA551 and BazarLoader

October 2021 – [IBM X-Force Reports](#) Shathak brokering initial access on behalf of Conti ransomware affiliates

November 2021 – **sonyblueprint[.]com** is [reported by Unit42](#) in association with Shathak, BazarLoader and VNC, a remote desktop sharing protocol that precedes RDP.

January 2022 – **customsecurityusa[.]com** and **juniperengineer[.]com** reported by Unit42 in association with Shathak and IcedID

## **TR Botnet and IcedID**

---

June, 2021 – [Proofpoint notes](#) use of IcedID by both TA577 and TA551 (insert more common name of these groups)

December, 2021 – **bqtconsulting[.]com** is [reported by SANS](#) in association with IcedID and the backdoor, DarkVNC

January, 2022 – **driverpackcdn[.]com** is [reported by Unit42](#) in association with IcedID

February 2022 – TRU observes two cyber incidents leveraging Cobalt Strike via the infrastructure (defined by the traits outlined in the Syndicate Infrastructure paragraph) on recently created domains. IcedID was the initial access vector.

## **Glossary of terms**

---

**IcedID** – a botnet loader known to arise from malicious documents and often leading to Cobalt Strike or other backdoors that position threat actors for ransomware deployment.

**TR Botnet (akaTA577)**– The TR botnet delivers payloads via malicious documents. TR has been associated with SquirrelWaffle and Qakbot campaigns but has recently been observed delivering IcedID.

**Shathak (aka TA551)**– A cybercrime group that is known for launching phishing campaigns that typically distribute malicious documents which, in turn, often lead to backdoors such as IcedID.

**Emotet** – A loader malware delivered via malicious document through email. Known to deliver Trickbot and Cobalt Strike.

**Trickbot** – A botnet loader delivered via malicious documents.

**Conti (aka Grim Spider)** – A large and sophisticated group of ransomware developers and operators, known for compromising and disrupting the critical operations of healthcare organizations, 911 emergency services, municipalities, oil transportation and storage providers, electric companies, schools, IT service providers, food and pharmaceutical providers. Conti popularized the modern ransomware model with its original project, Ryuk, which was delivered via Emotet dropping Trickbot.

**Cobalt Strike** – An intrusion suite, billed as “adversary simulation” that has sophisticated evasion features, such as a malleable C2 and an injection kit, to deploy more tools throughout a victim’s IT environments.

**Discovery** – generally the first tactic threat actors take when they get hands-on keyboard in an environment. Discovery helps threat actors determine the kind of endpoint they’ve landed on and what kind of accounts they can pivot too next.

**Lateral Tool Transfer** – a technique that allows an active intruder to import more intrusion tools from their own environment to the victims, including password crackers, exploits and exfiltration tools.

**Privilege Escalation** – allows attackers to raise privileges on a compromised account or obtain credentials for more privileged accounts.

**Malleable C2** – allows threat actors to rotate through different communication procedures, making it harder to track and detect known procedures.

**Artifact Kit** – a Cobalt Strike feature that allows an active intruder the ability to inject tools into legitimate windows processes, reducing their chance of detection.

**Initial Access** – how an intruder gains entry into a victim’s network. Examples include phishing emails, remote exploits, and supply-chain attacks.

**Aggressor Scripts** – It is a scripting framework, built within Cobalt Strike 3.0 and later versions, which will automate and customize the intrusion workflow being conducted by threat actors. Examples of Aggressor Scripts include notifying the threat actors of a successful compromise via Slack or running Mimikatz within the victim’s IT environment. Mimikatz is a credential password stealer tool.

**Beacon**—it is the Cobalt Strike’s backdoor.

**Beacon Profiles** –Beacon profiles define the configuration of the Beacon Backdoor—including the windows processes (aka injection targets) that **artifact kit** will use to deploy tools, how often Beacon will check in with Team Server, and the C2’s URL and port.

If you’re not currently engaged with a Managed Detection and Response provider, we highly recommend you partner with us for security services to disrupt threats before they impact your business. Want to learn more about how we protect organizations globally? [Connect](#) with an eSentire Security Specialist.

## Skip To:

---

- Burning a Conti Affiliate’s Cobalt Strike Infrastructure
- Cobalt Strike at Scale
- Why has Cobalt Strike become so popular for ransomware campaigns?
- Ransomware Operations Utilizing the Cobalt Strike Infrastructure
- Excerpt of the Cobalt Strike C2 Domain Names and IP Addresses Utilized by a Conti Affiliate
- The Cobalt Strike ShadowBeacon Incident
- Glossary of terms