# Case Study: Incident Response is a relationship-driven business

By Jonathan Munshaw

Published: 2021-05-17 · Archived: 2026-04-05 15:02:02 UTC


## Case Study: Incident Response is a relationship-driven business

Monday, May 17, 2021 08:00

## Proof that incident response is "the ultimate team sport"


*By [Brad Garnett](#).*

## Introduction

As a seasoned incident responder, and now IR business leader here at Cisco Talos Incident Response (CTIR), I have always said that incident response is the ultimate team sport. People are building blocks for organizations — and an effective incident response is about people, relationships and leveraging those relationships into the incident response workflow (processes and security instrumentation). This all plays a part in effectively containing and eradicating a determined adversary from the organization's network environment.

To highlight this, I want to share a recent CTIR engagement that shows how we can work together with an organization's IR and IT teams to quickly contain and remediate a threat. In this case, we dealt with an adversary that could critically affect a business by deploying ransomware and virtually completely shutting down their network. One of my favorite parts about my role with CTIR is the customer relationships I get to build around the world by leveraging our awesome Cisco Secure collaboration technology to work from anywhere and at home during the pandemic. I hear first-hand about the challenges and successes our customers have facing today's most challenging threats.

This customer case study I am going to highlight is a publicly traded company with more than $8 billion in revenue. This incident was even more complicated because the company was going through a merger and acquisition when the customer CISO received a phone call from my organization. This customer had an existing IR retainer with us and has a strong relationship with my organization — to the extent that we are viewed as an extended team. We notified this customer after we identified suspicious Cobalt Strike activity and TTPs consistent with pre-ransomware activity via SecureX telemetry.

> *"Our Cisco Talos partners recognize the critical role relationships play in cybersecurity and Incident Response. The Talos Team has invested significant time and effort in us to fully understand our people and environment before an incident occurred. Together, we built familiarity and trust between our teams that can only be obtained through constant engagement and drills. When we were faced with a significant security incident, that trust and familiarity were the key differentiators that enabled us to successfully contain the threat and minimize damages," customer CISO.*

## Initial notification

During the initial notification, we supplied our customer with the specific hostname and indicators we contacted them about. Below is the initial Cobalt Strike beacon that we identified in global telemetry:

> cmd.exe executed powershell -nop -w hidden -encodedcommand <redacted_base64_string>

Followed by the following for command and control (C2):

> cmd.exe executed powershell -nop -w hidden -encodedcommand <redacted_base64_string>
>
> powershell.exe Connected to 95[.]174[.]65[.]241[:]4444

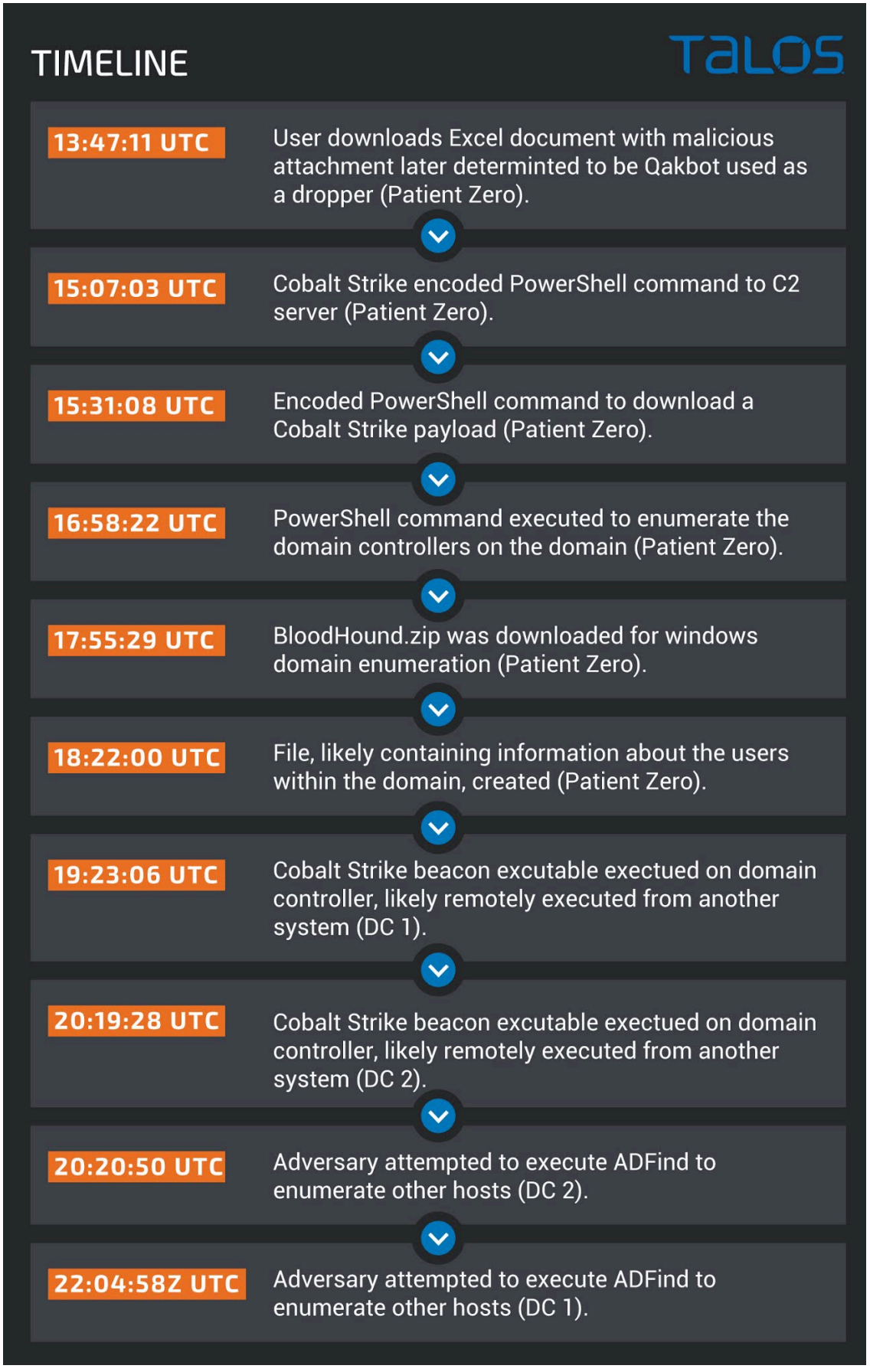
*Note: Please visit the Talos Reputation Center for accurate threat information.*

## Detection and analysis

This blog post will only highlight endpoint analysis, but the same approach was included in our analysis plan for the two compromised domain controllers.

Based upon our global SecureX telemetry and the customer's Cisco Secure Endpoint deployment, we were identified patient zero and focused our forensic analysis efforts on three key systems as part of our analysis plan:

1. Endpoint (Patient Zero): Windows 10 Enterprise 1909
2. Domain Controller 1 (DC1): Windows Server 2016 Standard
3. Domain Controller 2 (DC2): Windows Server 2012 R2 Standard




## Patient zero (Windows 10 endpoint)

### ATT&CK Technique with Sub-Technique (T1204.002) User Execution: Malicious File

Forensic analysis of the patient zero endpoint found that the file Document_1223672987_11142020.zip was downloaded to \Users\%Compromised_User%\Downloads. The RecentDocs registry entry shows that the user opened the ZIP archive shortly after the file was downloaded. Analysis of the Excel document contained within Document_1223672987_11142020.zip showed a malicious macro that was set to execute once the document was opened. This macro attempted to download a payload from "http[:]//redacted[.]com/bpebqznfbkgl/55555555555.jpg". This payload was then stored on the system in the "C:\IntelCompany" folder and executed using the rundll32 executable. The analysis also shows that the payload delivered by this document is the Qakbot banking trojan. The user was not warned of the macros existence before it was executed because this host was configured to trust all macros and all Excel documents from the internet.

| Registry Value Path | Value Data | Value Summary |
|---|---|---|
| HKCU\Software\Microsoft\Office\16.0\Excel\ Security\VBAWarnings | 1 | A value of 1 corresponds to the "Enable all macros" setting. This setting allows macros to execute automatically if a document is not in the protected view mode. |
| HKCU\Software\Microsoft\Office\16.0\Excel\ Security\ProtectedView\ DisableInternetFilesinPV | 1 | A value of 1 indicates that files downloaded from the internet will not enter the protected view mode. |
| HKCU\Software\Microsoft\Office\16.0\Excel\ Security\ProtectedView\ DisableAttachmentsinPV | 1 | A value of 1 indicates that email attachments will not enter the protected view mode. |
| HKCU\Software\Microsoft\Office\16.0\Excel\ Security\ProtectedView\ DisableUnsafeLocationsinPV | 1 | A value of 1 indicates that documents within temporary directories will not enter the protected view mode. |

### ATT&CK Technique with Sub-Technique (T1059.001) Command and Scripting Interpreter: PowerShell

We observed multiple executions of Cobalt Strike beacon-encoded PowerShell payloads from the 'Compromised_User' user during the analysis of the Windows PowerShell event log.

| Execution Timestamp (UTC) | Payload Description |
|---|---|
| 2020-11-20T15:07:03Z | Cobalt Strike encoded PowerShell command that called out to XX.XXX.XX[.]XXX over port 80 |
| 2020-11-20T15:11:20Z | Cobalt Strike encoded PowerShell command that called out to XX.XXX.XX[.]XXX over port 443 |
| 2020-11-20T15:23:47Z | Cobalt Strike encoded PowerShell command that called out to XX.XXX.XX[.]XXX over port 8080 |
| 2020-11-20T15:26:05Z | Cobalt Strike encoded PowerShell command that called out to XX.XXX.XX[.]XXX over port 80 |
| 2020-11-20T15:31:08Z | Encoded PowerShell command to download a Cobalt Strike payload from http[:]//XX.XXX.XX[.]XXX:80/agel |
| 2020-11-20T15:43:45Z | Cobalt Strike encoded PowerShell command that called out to XX.XXX.XX[.]XXX over port 8080 |

Analysis of the encoded payloads revealed that the Cobalt Strike command and control traffic was configured to use the following user agents:

> Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.157 Safari/537.36
>
> Windows-Update-Agent/10.0.10011.16384 Client-Protocol/1.40

The PowerShell event log also showed that at 2020-11-20T16:58:22Z, the following PowerShell command was executed to enumerate the domain controllers on the domain:

```
powershell
[System.DirectoryServices.ActiveDirectory.Domain]::GetCurrentDomain().DomainControllers | Select -property Name,IPAddress,OSVersion
```

**ATT&CK Technique with Sub-Technique (T1087.002) Account Discovery: Domain Account**

**ATT&CK Technique (T1018) Remote System Discovery**

During analysis of the Master File Table ($MFT), we concluded that at 2020-11-20T17:55:29Z "20201120104627_BloodHound.zip", which was an archive containing an open-source tool known as BloodHound used for enumerating windows domains, was downloaded to the "\Users\Public" folder. At 2020-11-20T18:22:00Z, the file "20201120132133_users.json" was created in "\Users\%Compromised_User%\Downloads". Although the contents of the file were not included in the evidence collected, our assumption based upon supporting evidence is that this file is an output file from the execution of bloodhound containing information about the users within the domain. Similarly, at 2020-11-20T20:40:00Z the file "20201120132133_computers.json" was created in the "\Users\%Compromised_User%\Downloads" folder. We concluded with high confidence that this file contained BloodHound output with information about the hosts within the domain.

## Containment, eradication and recovery

The collaborative, joint incident response between the customer's IR team and CTIR led to a quick containment and full eradication of an active adversary in the enterprise IT environment that had the capability to deploy ransomware. During these phases of the incident response, there were various actions performed, including but not limited to, re-imaging the patient zero endpoint, password resets, and the deployment of additional GPOs to restrict document macros, PowerShell and SMB/ Admin Shares. In every incident response, there are lessons learned. This is how organizations continue to evolve defense and detection capabilities, threat models, and incident response plans and playbooks. If your organization is interested in any of these services, please reach out to CTIR for more information.

## Post-incident activity

During our post-incident briefing with this customer and its executive leadership, we commended the customer and their entire organization for their swift response and collaboration with CTIR to successfully contain and eradicate a determined adversary that likely would've caused millions of dollars in lost revenue and recovery expenses. I am humbled to share this joint success story, as a lot of IR organizations are summoned once

ransomware has been deployed and the entire organization has affected, which is something that we observe globally and across industry verticals in our quarterly IR trends.

## Conclusion

I am grateful for the mutual, high-trust relationship between this customer and my organization. Incident response is a relationship-driven business. CTIR retainers are critical for organizations to augment their IR capabilities. A tested incident response plan that accurately reflects your organization's current capabilities is critical, as evidenced in the two Case Studieswe released today. Organizational and third-party relationships are tested during a crisis. It's important that there is an elevated level of trust between IR team and client, and that there is an established and agreed-upon process when time is of the essence to prevent an enterprise-wide ransomware attack when adversary pre-ransomware activity is identified. CISOs and executives should review and refine third-party relationships on a routine basis. Have your third-party IR relationships been tried and tested — and are those relationships resilient?

If you want to learn more about CTIR, check out our website here and visit us at this year's virtual RSA Conference this week.

---