How IronNet's Behavioral Analytics Detect REvil and Conti Ransomware

ironnet.com/blog/ransomware-graphic-blog

Back to IronNet Blog

Threat Research

By IronNet Threat Analysis and Research Teams, including lead contributors Morgan Demboski, Joey Fitzpatrick, and Peter Rydzynski

Nov 16, 2021

Table of Contents

- REvil intrusion
- Conti intrusion

Earlier this year, the DFIR Report published two separate articles outlining ransomware attacks by Conti and REvil, both of which leveraged the IcedID trojan in their intrusions. Using the PCAP (Packet Capture) from these reports, IronNet replayed the intrusions in our proprietary testing environment to test how IronDefense and our behavioral analytics detect malicious activity by these groups.

REvil

To start, we'll dive in to REvil ransomware, how it traversed the network in this intrusion, and how our analytics detected this activity.

First observed in April 2019, REvil (aka Sodinokibi) is an infamous Russia-based cybercrime syndicate responsible for several notable attack campaigns, including the ransomware attacks against Kaseya and JBS Foods. Operating under a ransomware-as-a-service (RaaS) model, REvil was ranked first among the most common ransomware variants in the first half of 2021 with 14.2% of the total market share. In October 2021, REvil reportedly shut down its operations following the arrest of several of its members and the hijacking of its infrastructure by law enforcement.

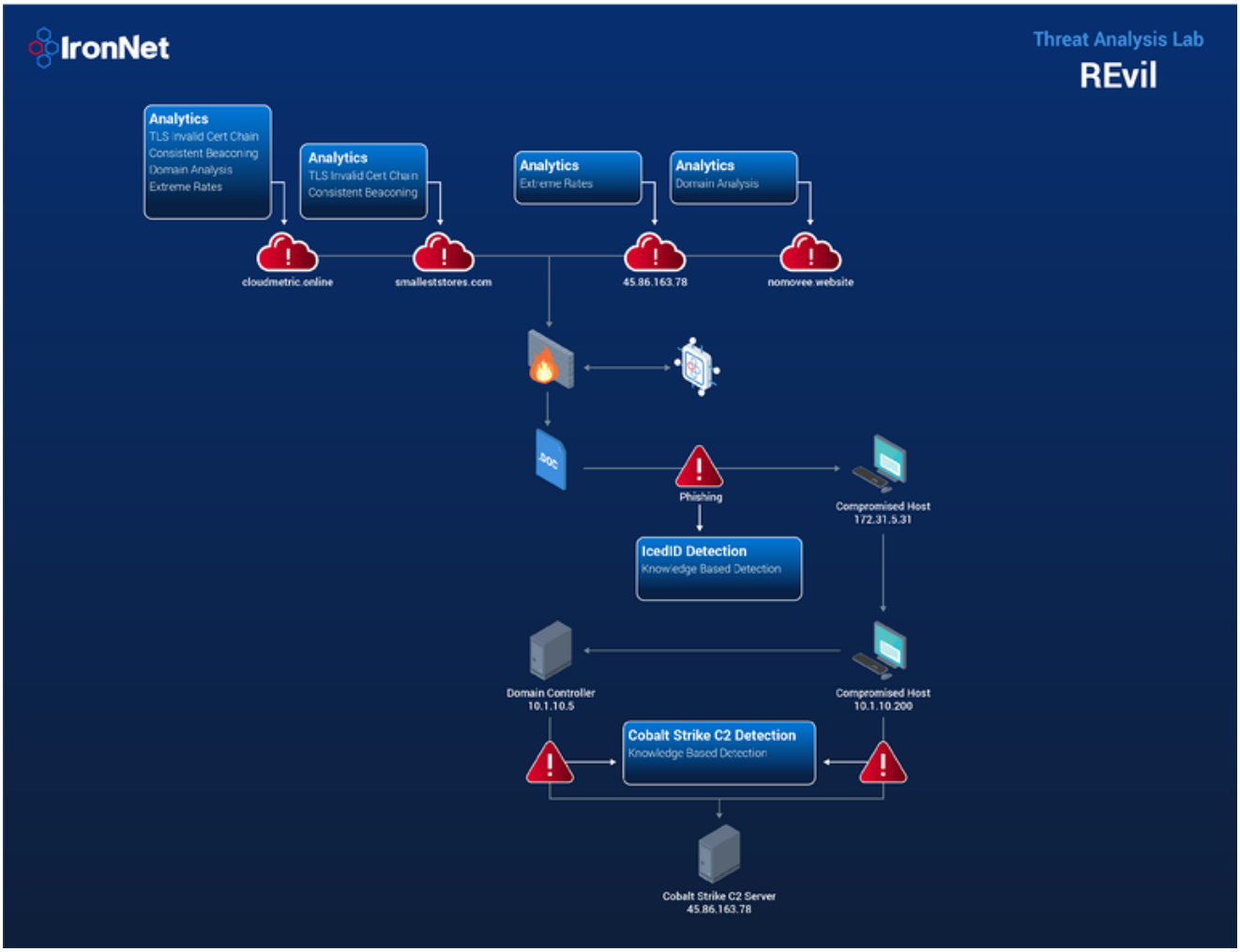


Figure 1: REvil malicious traffic and IronNet behavioral analytics

The threat actors begin with a malspam campaign to deliver a malicious XLSM file. Upon opening the macro, it initiates a WMIC (Windows Management Interface Command) command that executes IcedID from a remote executable posing as a GIF. The initial compromised host (172.31.5.31) downloads the malicious file hosting IcedID, which is flagged by our knowledge-based rules.

IronNet's knowledge-based detection uses Suricata rules to analyze netflow and detect common malicious behavior. Knowledge-based detection is an integral part of defense-in-depth and allows us to flag known indicators. However, it's important to note that signature-based detection should not be used alone when defending against ransomware, because cybercriminals take incredible care to avoid reusing IOCs (e.g. domains, IPs, file hashes, etc.) in an effort to evade signature detection.

As IcedID is downloaded to the host and executed using rundll32.exe, our Consistent Beaconing TLS analytic fires on the nomovee[.]website domain. Our Domain Analysis analytic is also alerted on the nomovee[.]website domain.

The Consistent Beaconing analytic analyzes beacon activity to detect ongoing patterns of both periodic and randomized beaconing, identifying when there is activity consistent with repetitive attempts by malware to establish communications with a C2 server.

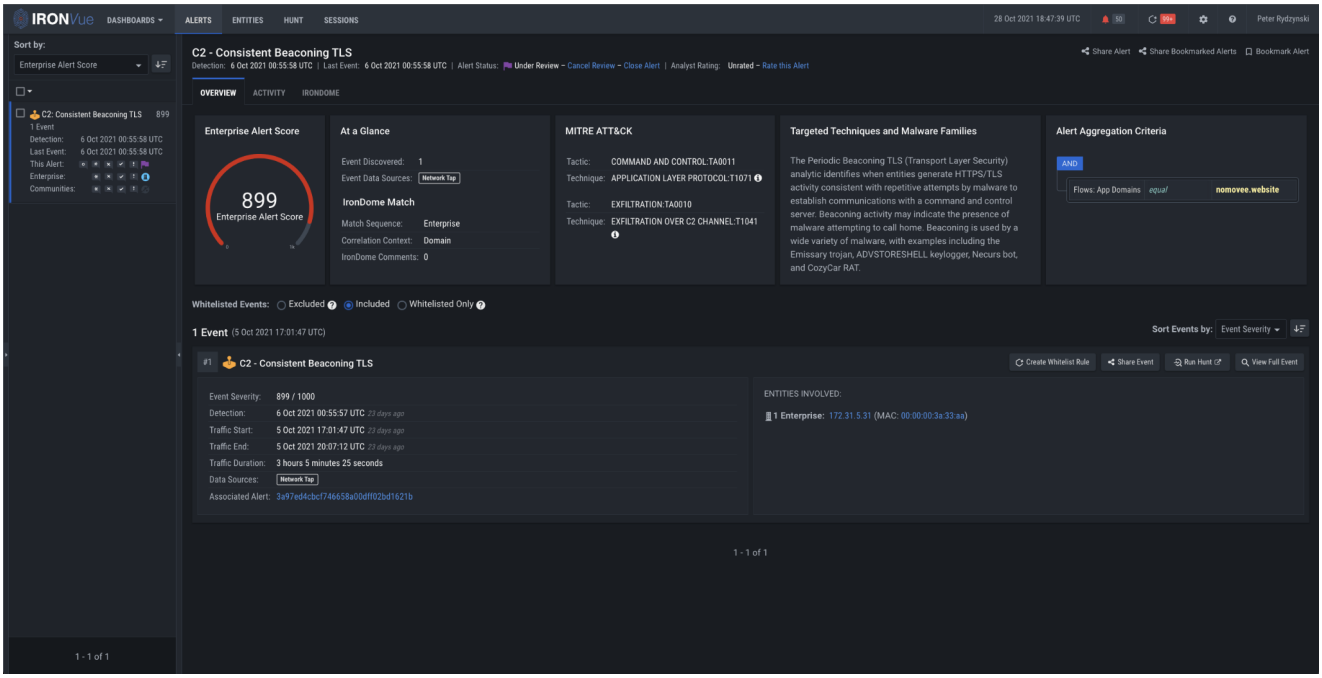


Figure 2: Consistent Beaconing TLS analytic firing on nomovee[.]website

It is from here that IcedID pulls down Cobalt Strike Beacons from two different command-and-control (C2) servers: cloudmetric[.]online (45.86.163.78) and smalleststores[.]com (195.189.99.74). On both of these, our TLS Invalid Certificate Chain analytic fires detecting suspicious TLS certificate usage.

A wide variety of malware may exhibit invalid TLS certificate chain behavior as part of C2 or even data exfiltration activities. IronNet's TLS Invalid Certificate Chain analytic assesses the TLS certificate to identify self-signed or falsified TLS certificates, validating all available server certificate chains in a flow and generating events for chains that fail the validation process – such as it did in this case.

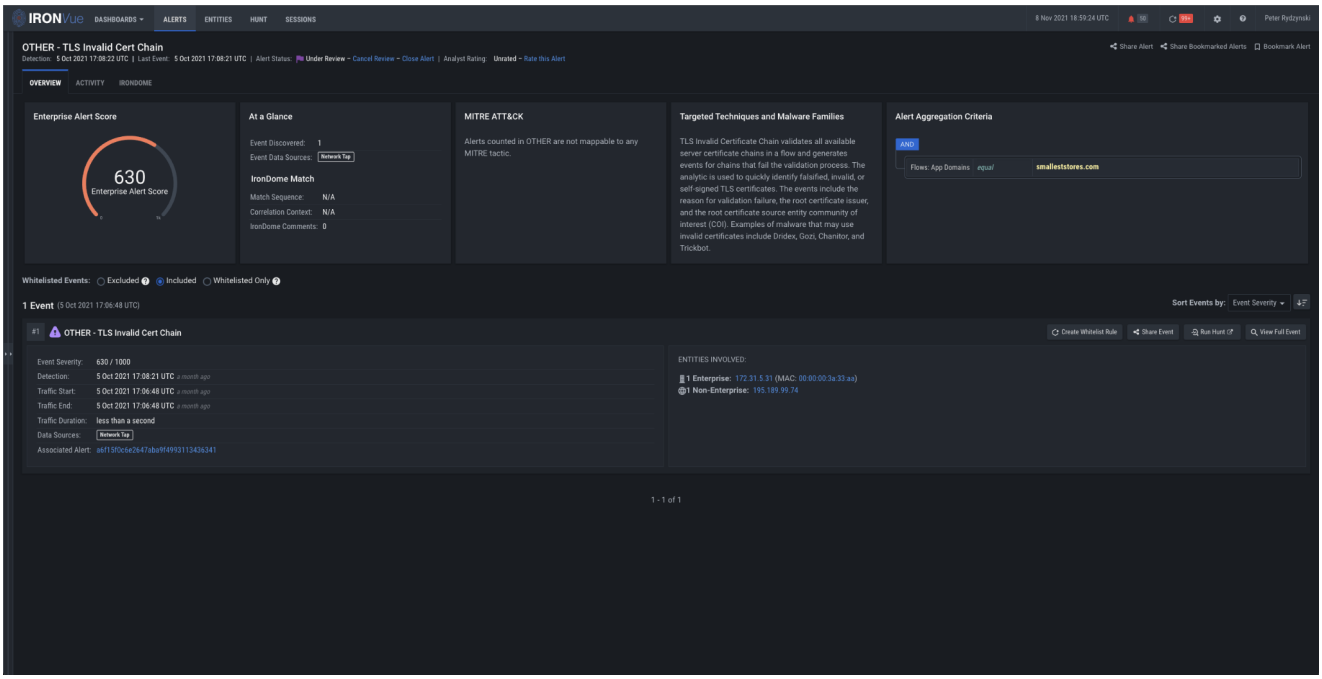


Figure 3: TLS Invalid Cert Chain analytic firing on smalleststores[.]com

Additionally, we have a Domain Analysis alert to support the finding for cloudmetric[.]online.

IronNet's Domain Analysis analytic evaluates outgoing communications from an internal host to a new or unusual domain, which could be the result of malware calling back to a domain for instructions. Given the nature of modern networks and their reliance on domains for communication, our Domain Analysis analytics provides value through the entire attack chain.

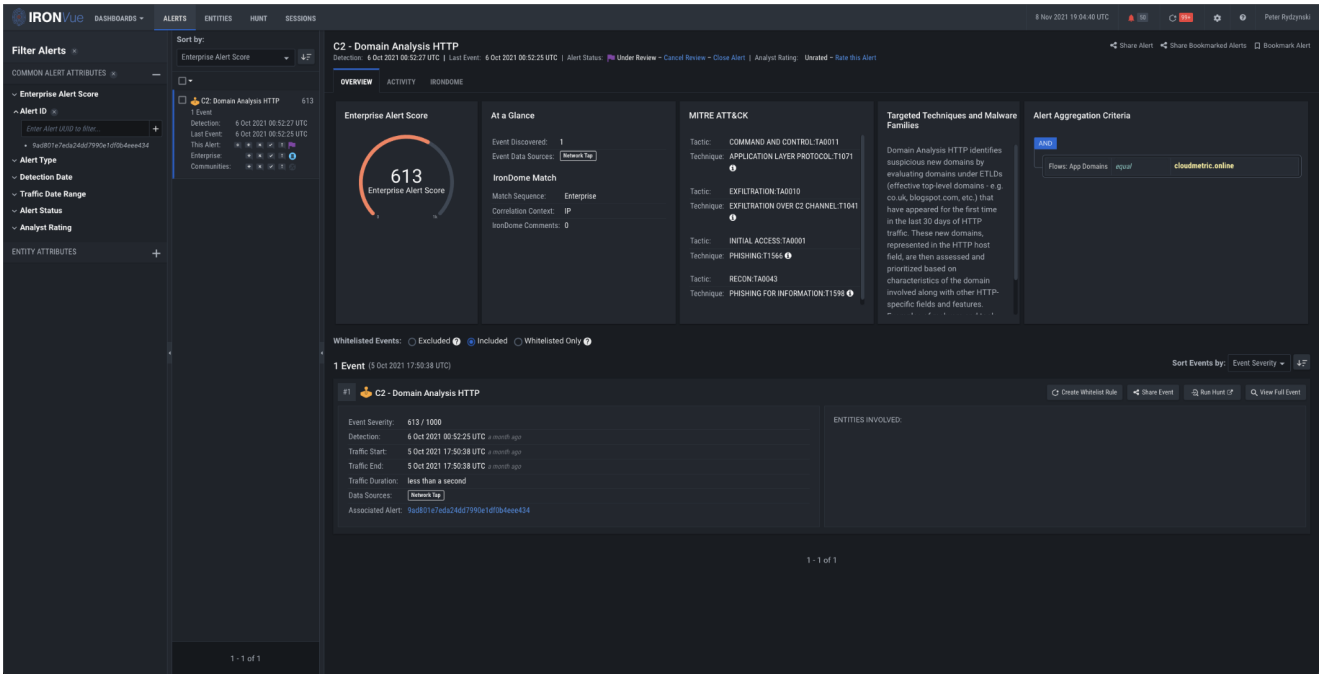


Figure 4: Domain Analysis HTTP analytic firing on cloudmetric[.]online

After establishing C2, the host begins to beacon consistently to the malicious domains. C2 communications are an integral part of a ransomware attack, especially given recent trends where ransomware operators look to fully enumerate networks, ultimately trying to achieve full domain compromise. Our beaconing analytics were designed to catch these types communications, which they did for cloudmetric[.]online and smalleststores[.]com.

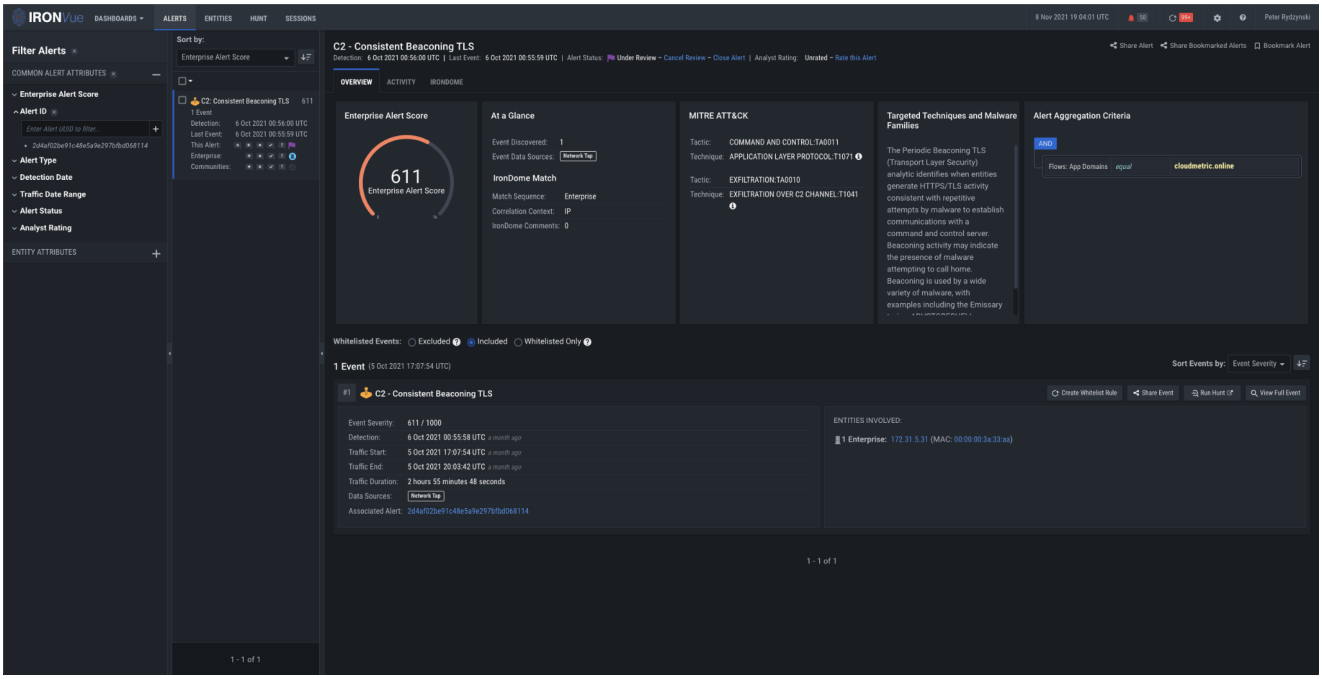


Figure 5: Consistent Beaconing TLS analytic firing on cloudmetric[.]online

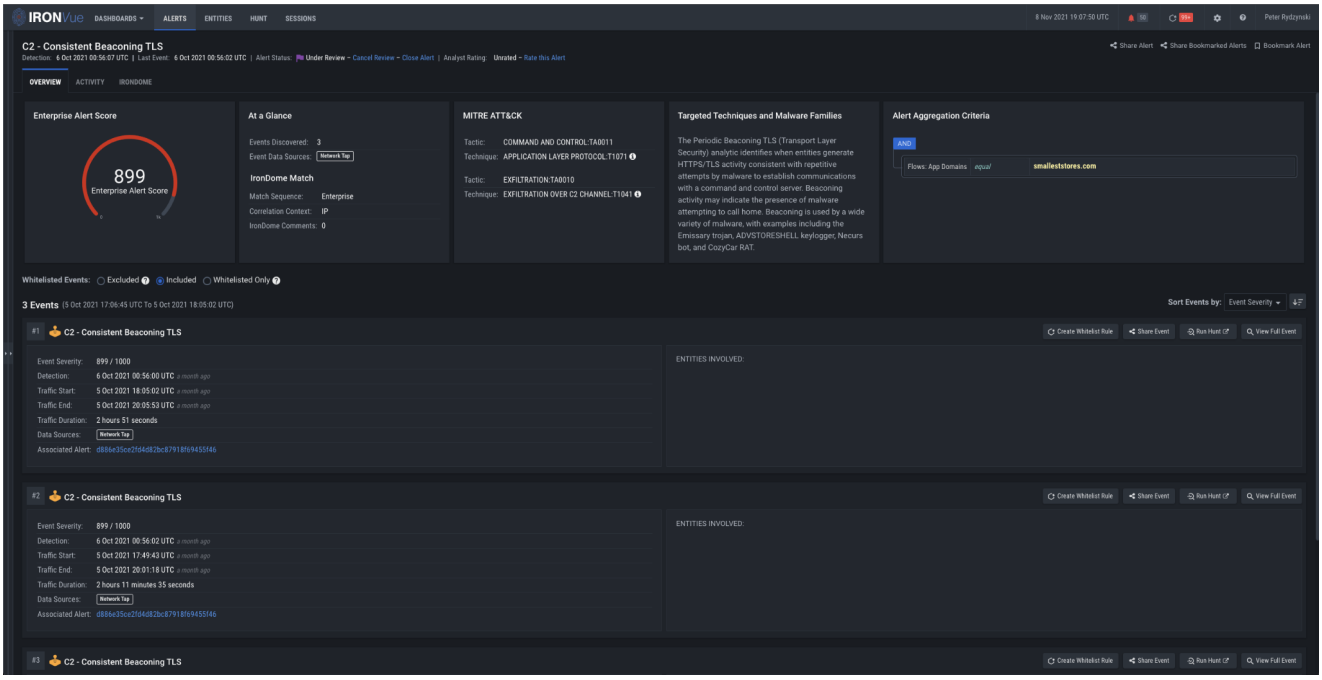


Figure 6: Consistent Beaconing TLS analytic firing on smalleststores[.]com

Using Cobalt Strike, lateral movement begins first to an Exchange server. After compromising the Exchange server, the threat actors move to domain controllers (DCs) and other servers within the environment using Server Message Block (SMB) and Cobalt Strike Beacons that are executed via a remote service. From the DCs, the attackers carry out additional discovery by using ADFind and the Ping utility to examine connections between the DCs and other domain-joined systems.

It was here that our knowledge-based rules detected the primary DC (10.1.10.5) and the internal Windows host (10.1.10.200) communicating with the Cobalt Strike C2 (45.86.163.78).

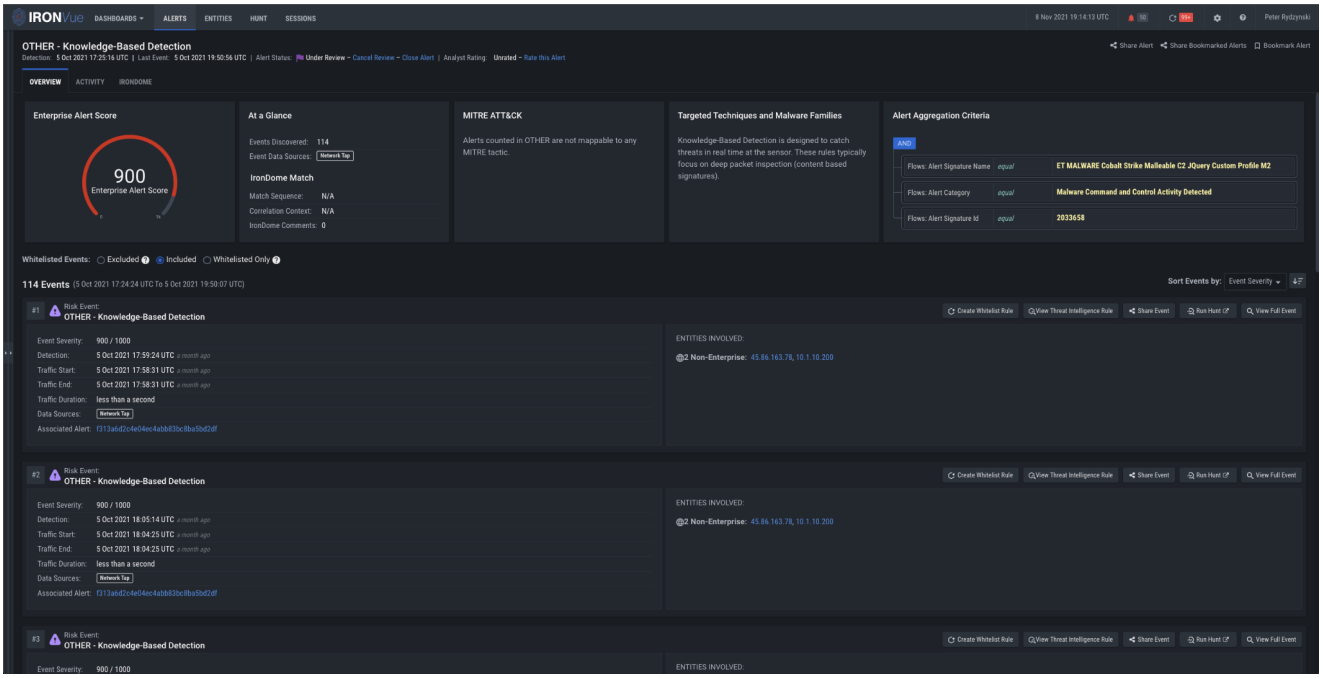


Figure 7: Knowledge-based detection of C2 communications between 10.1.10.200 & 45.86.163.78

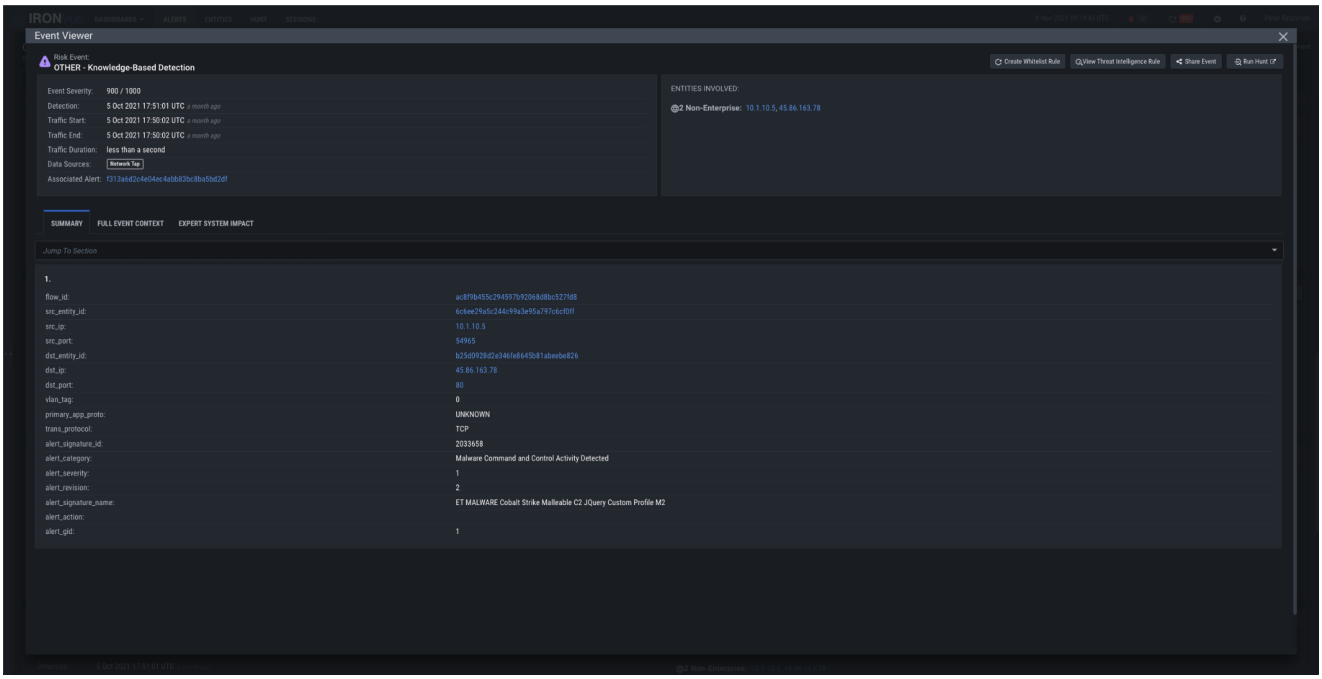


Figure 8: Event summary of knowledge-based detection of C2 communications between 10.1.10.5 & 45.86.163.78

Following this, the attackers used a Cobalt Strike beacon to dump credentials on the server and DC. The threat actors began to establish RDP (remote desktop protocol) connections between various systems. From here, the attackers used Rclone to exfiltrate files they will leverage in a double-extortion demand. As this occurs, our Extreme Rates analytic fired on 45.86.163.78 and cloudmetric[.]online.

IronNet's Extreme Rates analytic monitors traffic characteristics – such as the number of bytes, packets, and flows in network peer groups – to detect when a larger-than-normal amount of data is being extracted from the network. This presents an opportunity for detection before encryption can kick off. Some damage may still occur if an attacker is able to reach this point, but detecting and eradicating a threat at this stage is still immeasurably better than after encryption occurs.

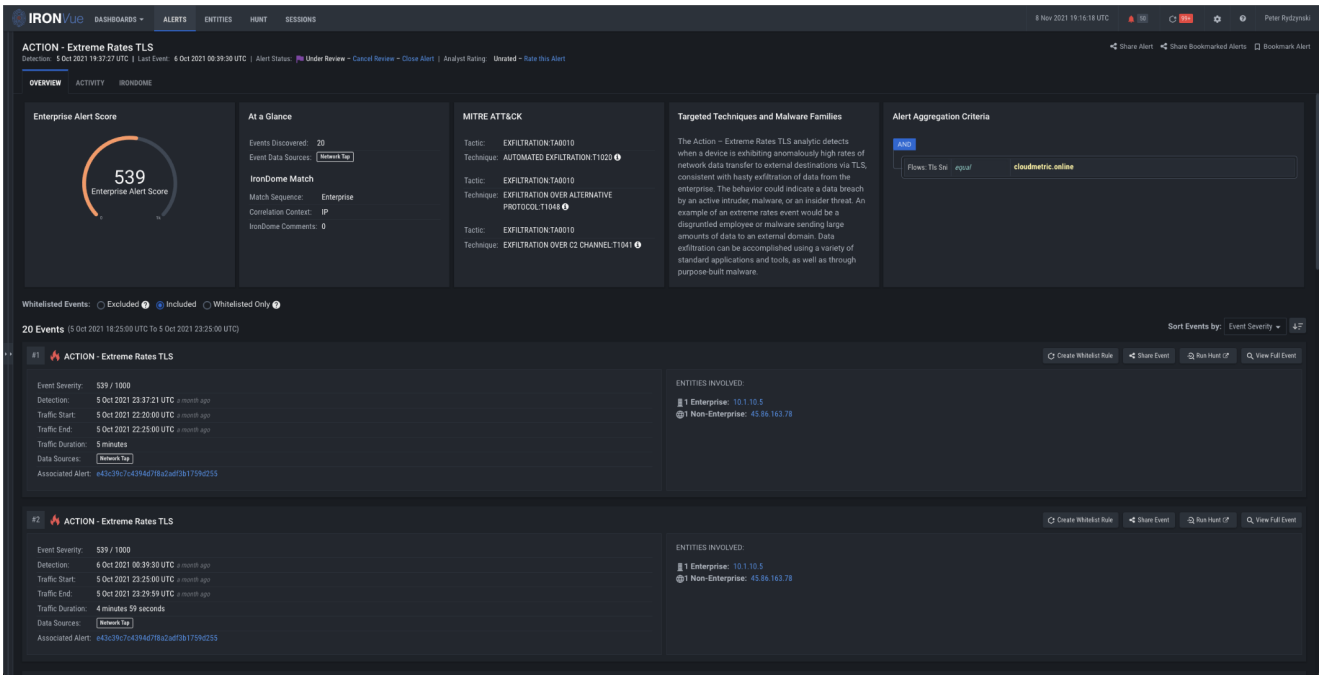
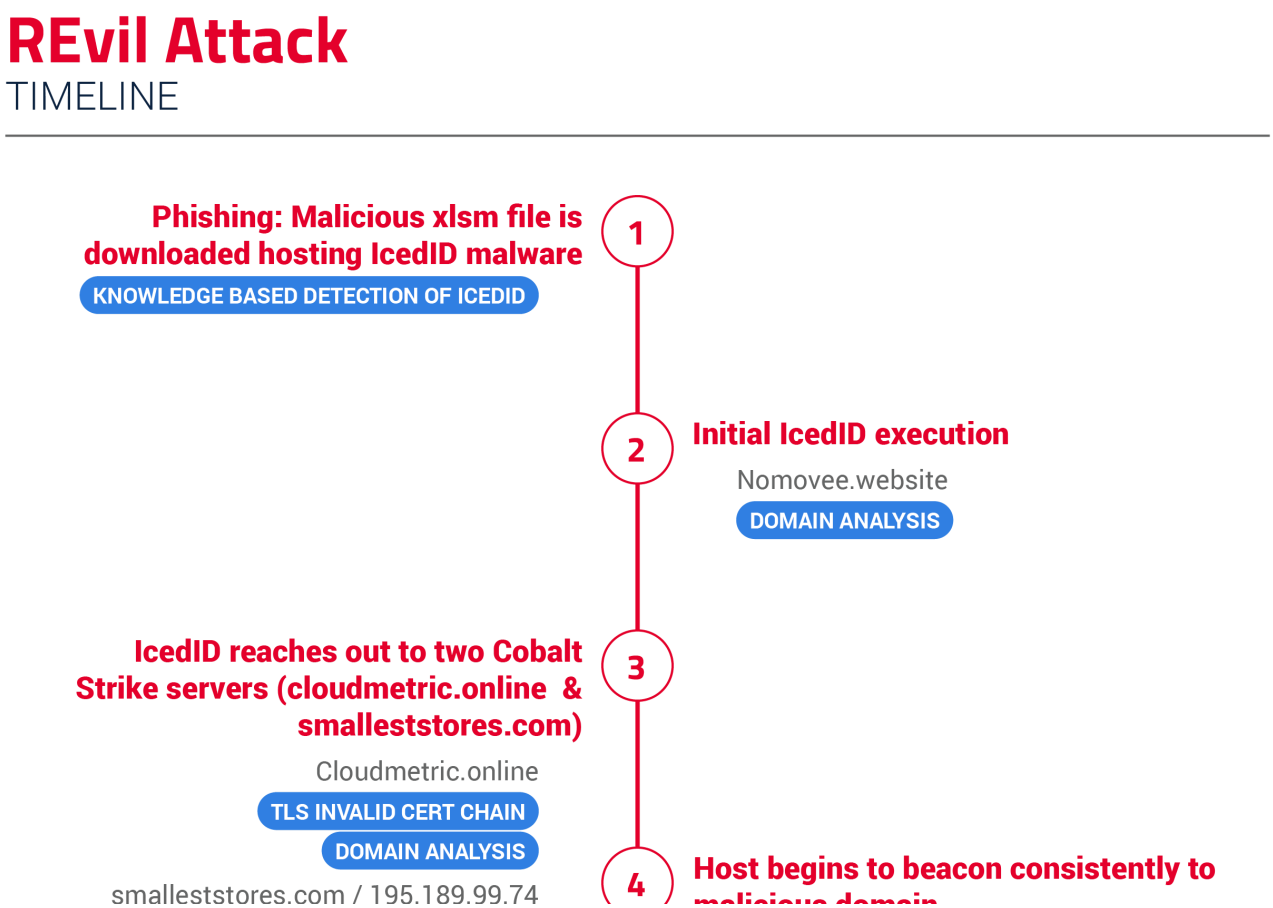
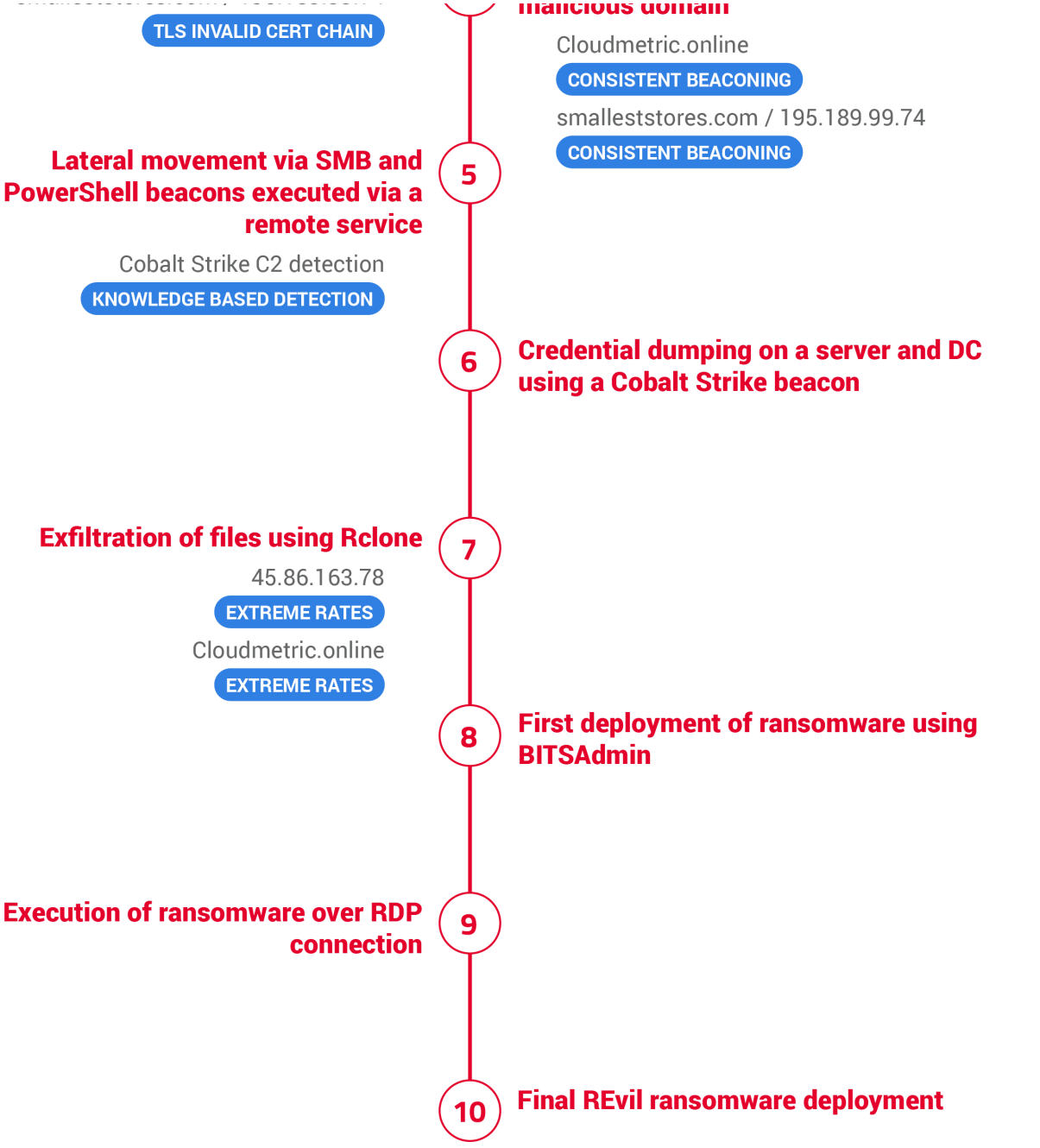


Figure 9: Extreme Rates TLS analytic firing on cloudmetric[.]online

The attackers then start to move onto final objectives, staging the executable on a DC and then using BITSAdmin to distribute it to each system in the domain. The ransomware is executed over an RDP connection, leading all domain-joined systems to be encrypted.





Conti

Let's now dive in to Conti, how it traversed the network in this intrusion, and how our analytics detect this activity.

Conti is a prolific ransomware family that first emerged in May of 2020. The group garnered particular attention in 2021 for several cyberattacks on healthcare institutions, including the Ireland Health Service Executive (HSE). Overall, Conti has been connected by the FBI to

more than 400 cyberattacks worldwide – 75% of which targeted organizations in the U.S.

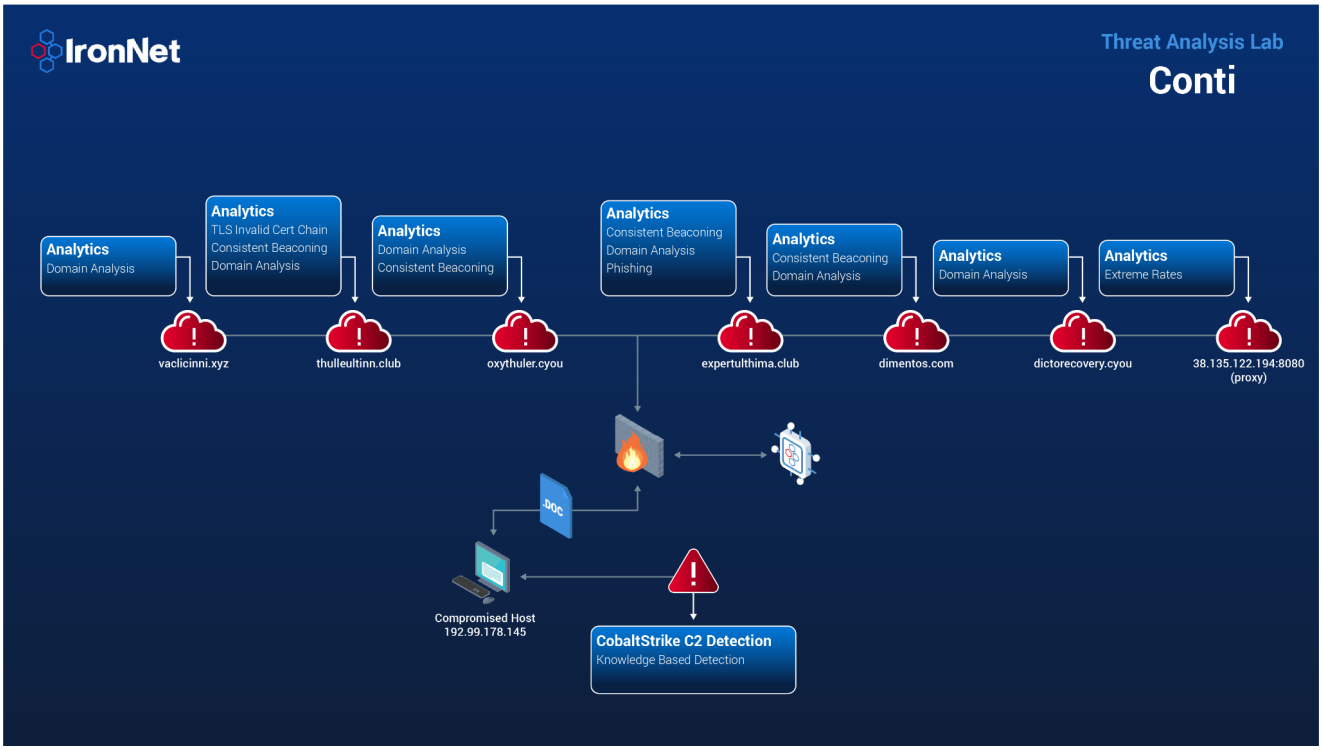


Figure 10: Conti malicious traffic and IronNet behavioral analytics

The attackers begin with a phishing campaign delivering a Zip file that contains a malicious Javascript file. Our Phishing HTTPS analytic catches this interaction with the phishing link and fires on expertulthima[.]club.

IronNet's Phishing HTTPS analytic analyzes all SSL/TLS encrypted communications from internal devices to external domains, the SNI (Server Name Indication), and the certificate of the destination to identify communications with phishing domains employing targeted brand imitation via HTTPS. Our analytics are not isolated to just email-based phishing, but also identify any time a user appears to be interacting with a phishing link or submitting sensitive information to a suspicious external entity.

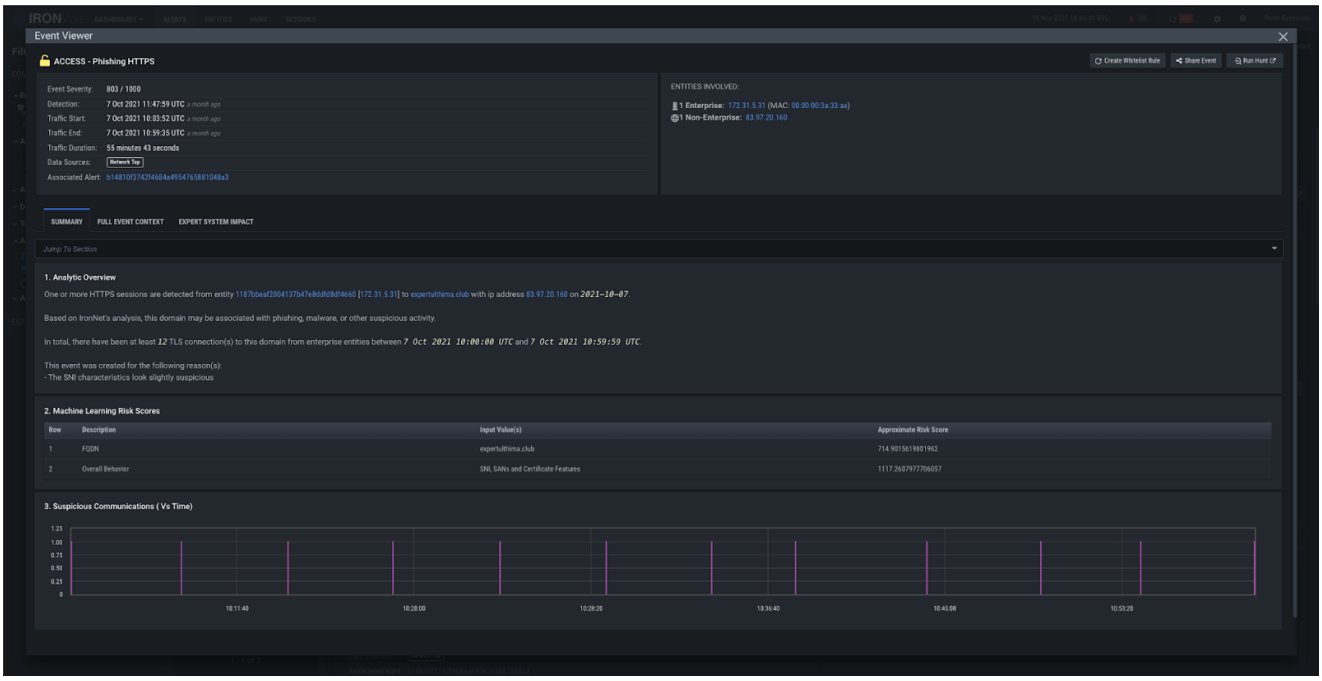


Figure 11: Phishing HTTPs analytic firing on expertulthima[.]club

The file eventually downloads and executes the IcedID trojan via rundll32.exe. In the initial IcedID execution, our Domain Analysis analytic fires on vaclicinni[.]xyz, dictorecovery[.]cyou, oxythuler[.]cyou, Thulleultinn[.]club, and Expertulthima[.]club.

IronNet's Domain Analysis analytic monitors outgoing communications, and it provides unique value as it does not rely on the existence of any additional behaviors, just the usage of a suspicious domain.

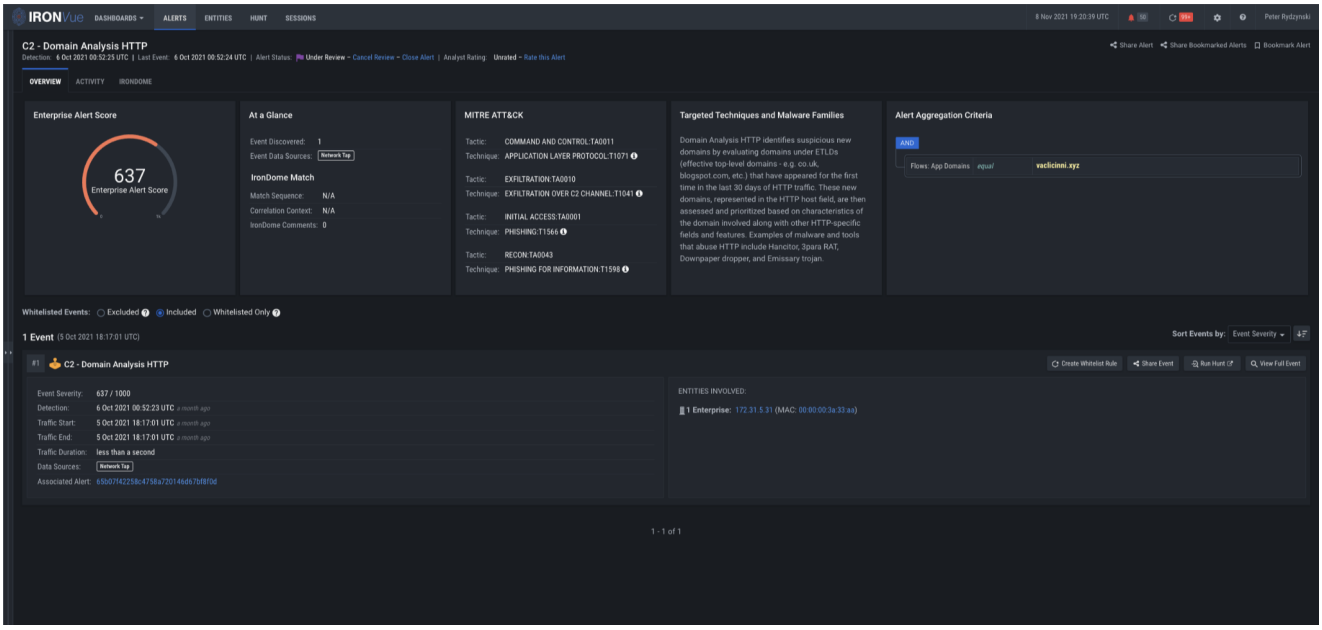


Figure 12: Domain Analysis HTTP analytic firing on vaclicinni[.]xyz

In addition to Domain Analysis, our Consistent Beaconing analytic fired for oxythuler[.]cyou, Thulleultinn[.]club, and Expertulthima[.]club, and our TLS Invalid Certificate Chain analytic fired for oxythuler[.]cyou and thulleultinn[.]club.

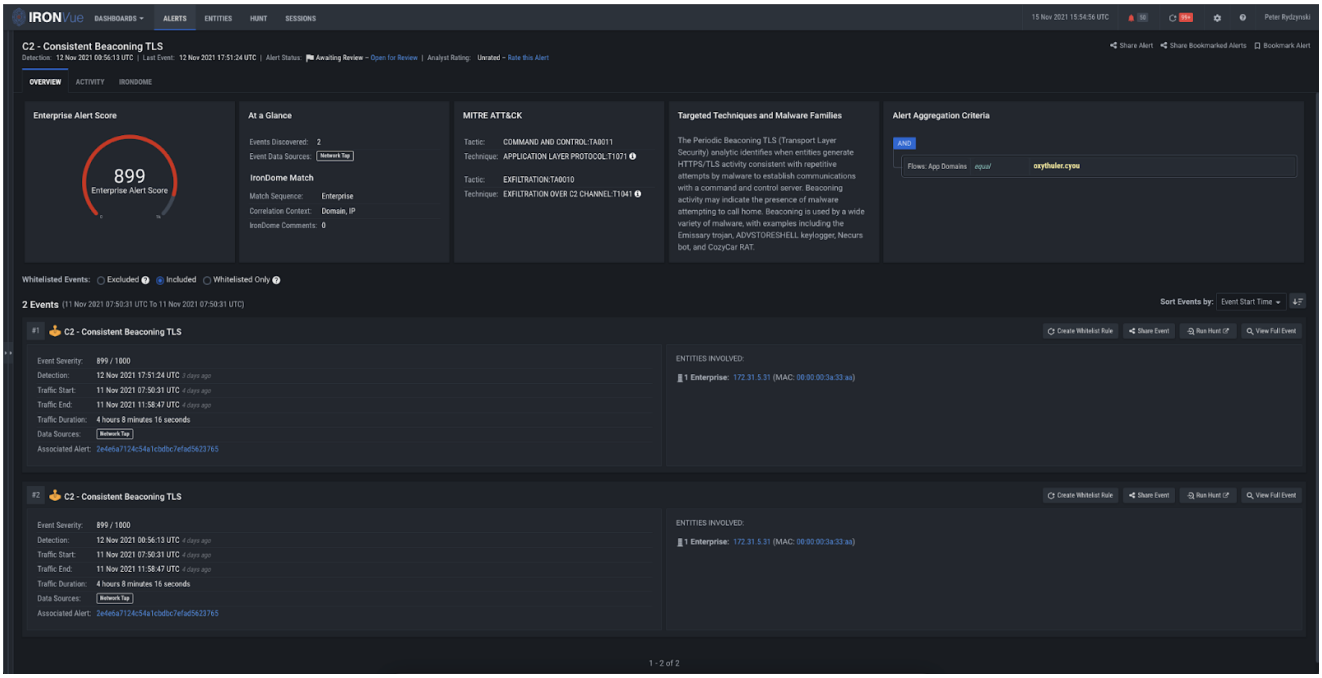


Figure 13: Consistent Beaconing TLS analytic firing on oxythuler[.]cyou

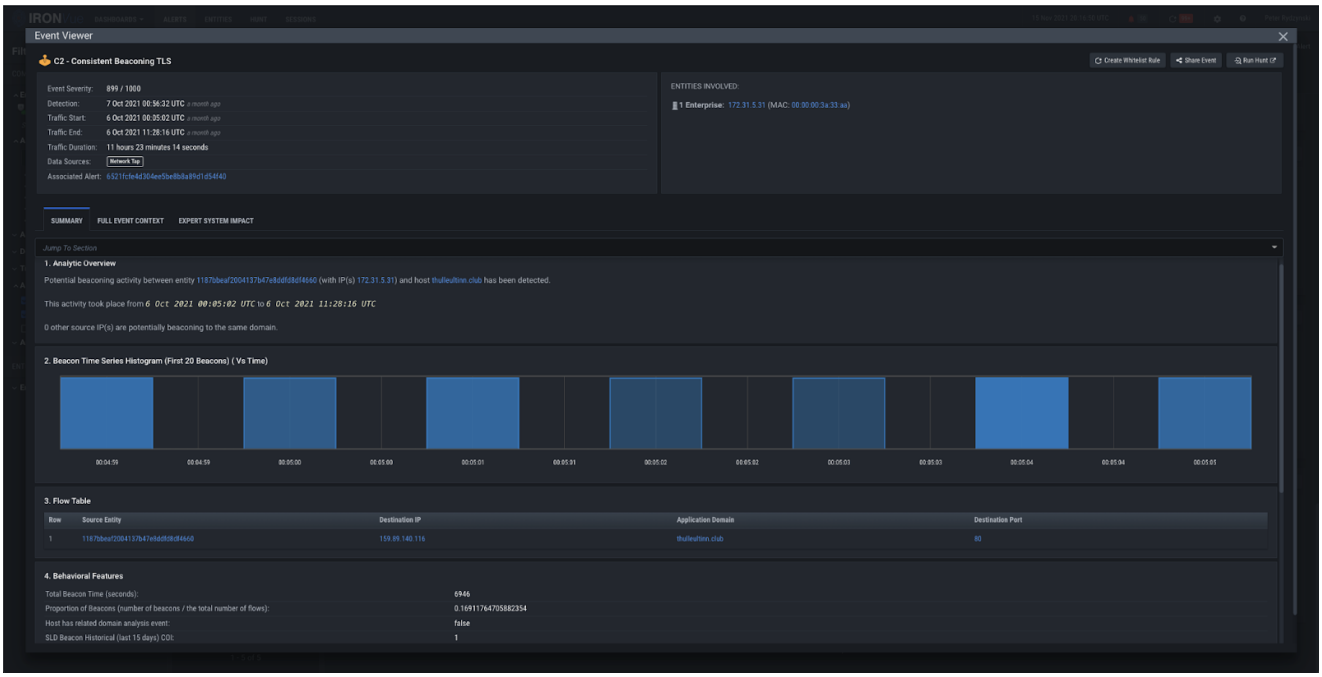


Figure 14: Consistent Beaconing TLS analytic firing on thulleultinn[.]club

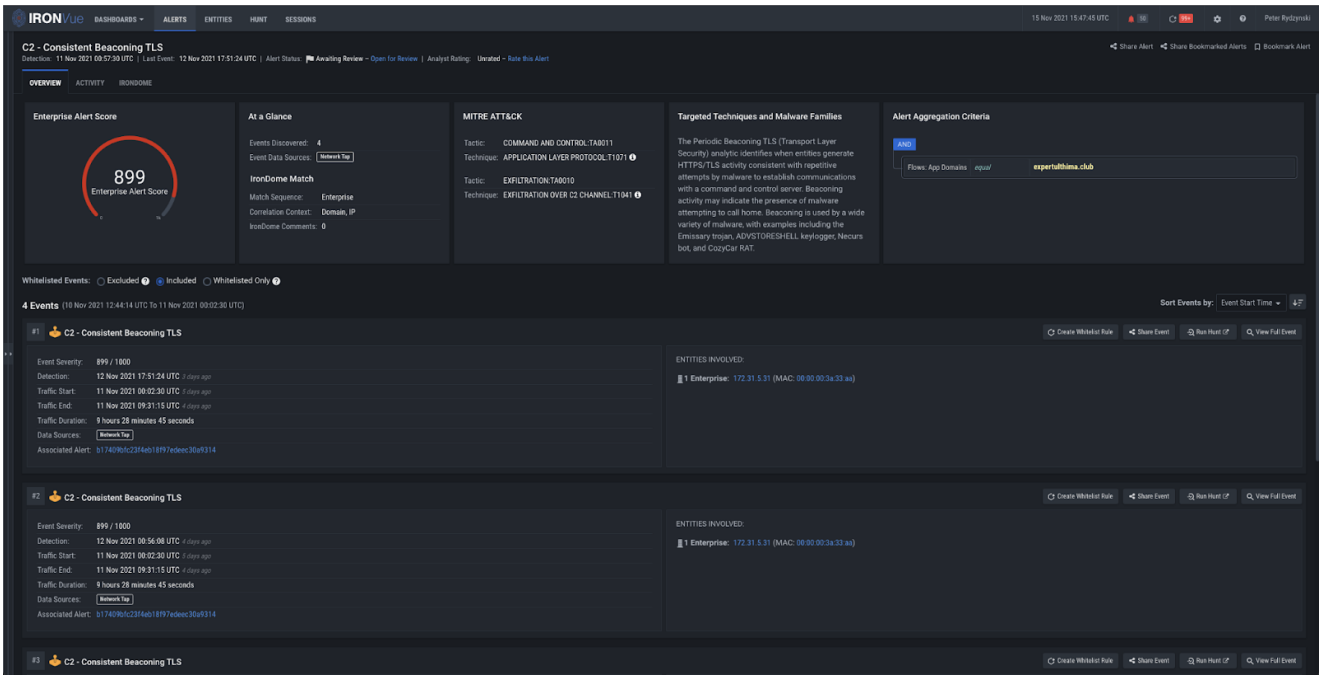


Figure 15: Consistent Beaconing TLS analytic firing on expertulthima[.]club

The TLS Invalid GCertificate Chain analytic validates all available server certificate chains in a flow and generates events for chains that fail the validation process. The events include the reason why validation failed, the root certificate issuer, and the number of internal devices that are communicating with the device issuing the root certificate.

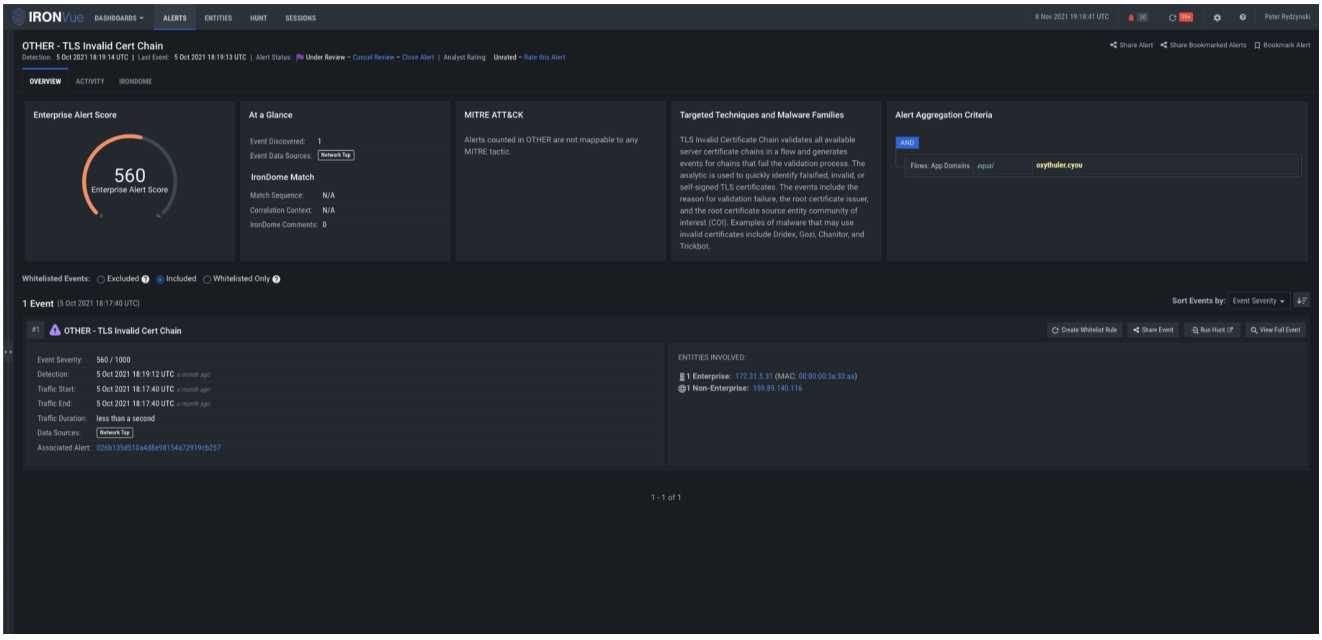


Figure 16: TLS Invalid Cert Chain analytic firing on oxythuler[.]cyou

Once the attackers successfully infect the system with IcedID, they drop and execute a Cobalt Strike beacon. At this point, our knowledge-based rules fire to detect Cobalt Strike C2 (192.99.178.145).

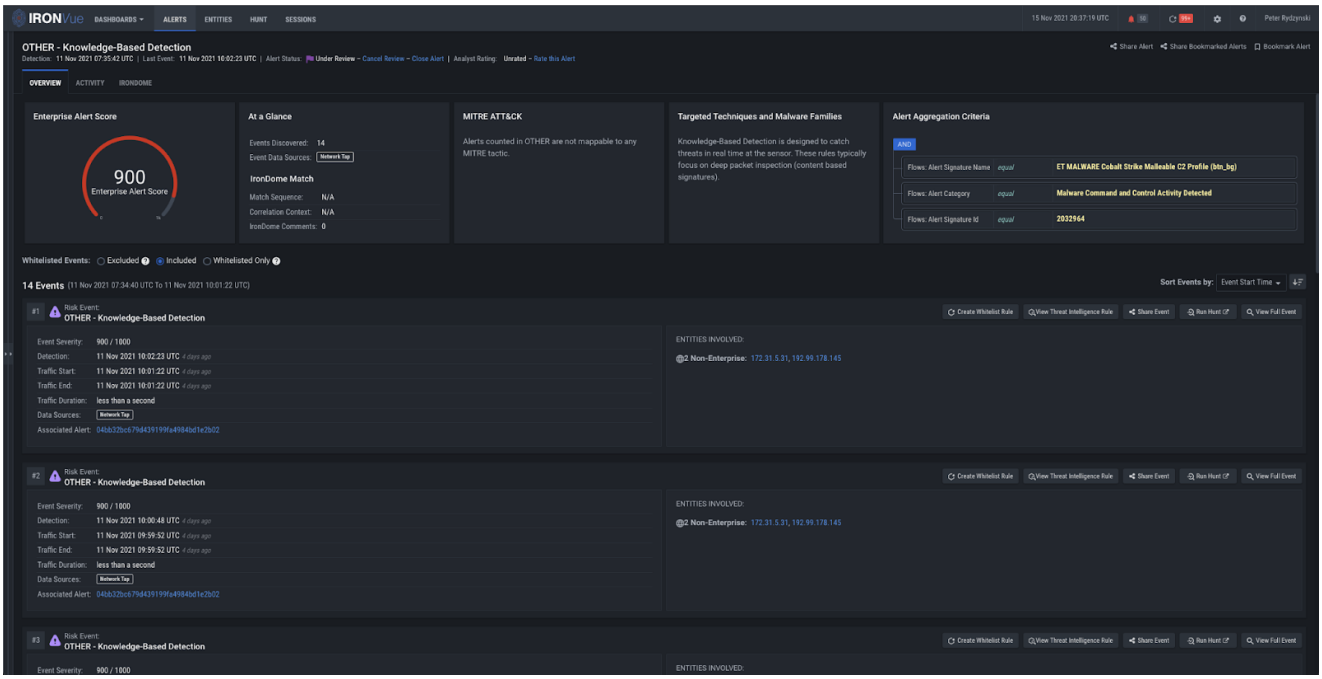


Figure 17: Knowledge-based detection of Cobalt Strike C2 (192.99.178.145)

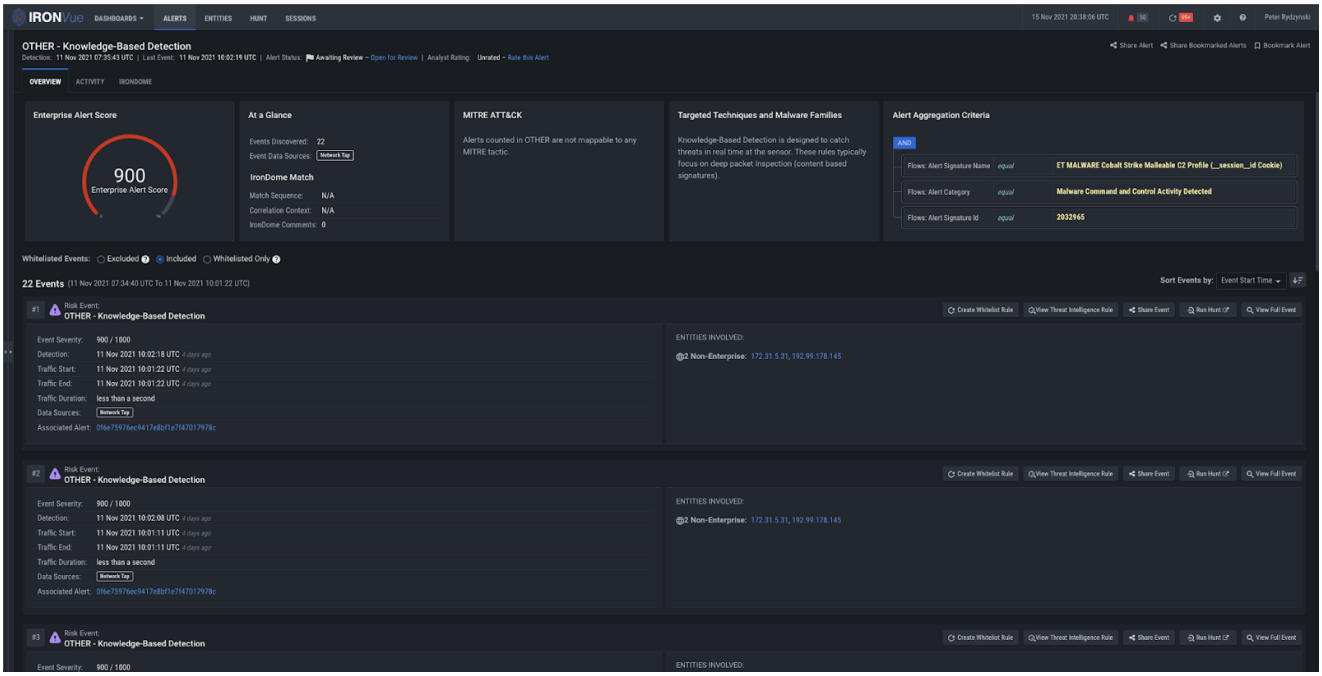


Figure 18: Knowledge-based detection of Cobalt Strike C2 (192.99.178.145)

The attackers then perform domain enumeration using native Windows tools such as nltest.exe, whoami.exe, and net.exe. They escalate to SYSTEM privileges via Cobalt Strike's built-in "named pipe impersonation" functionality.

Moving laterally to the DCs, the threat actors utilize SMB to transfer and execute a Cobalt Strike Beacon. During this, one of the DCs conducts port scanning activity to identify open ports. Afterward, the threat actors transfer a Cobalt Strike DLL (Dynamic Link Library) to

Admin shares and distribute it throughout the environment using PsExec. Our Consistent Beaconing and Domain Analysis analytics fire for the Cobalt Strike C2 domain dimentos[.]com.

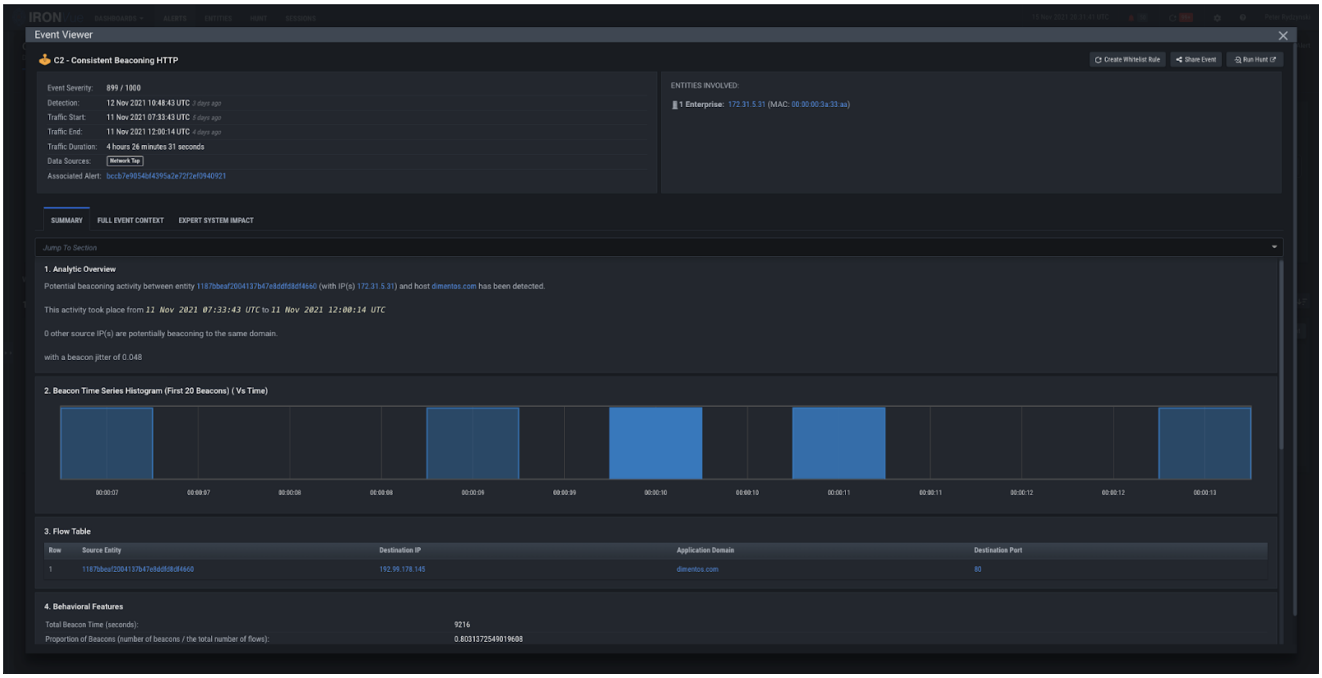


Figure 19: Consistent Beaconing HTTP analytic firing on dimentos[.]com

Later on, the attackers establish RDP connections to the DC and other systems throughout the environment. To do this, they use a redirector (38.135.122.194) to proxy the RDP traffic passing through the IcedID process. This activity was caught by our Extreme Rates analytic.

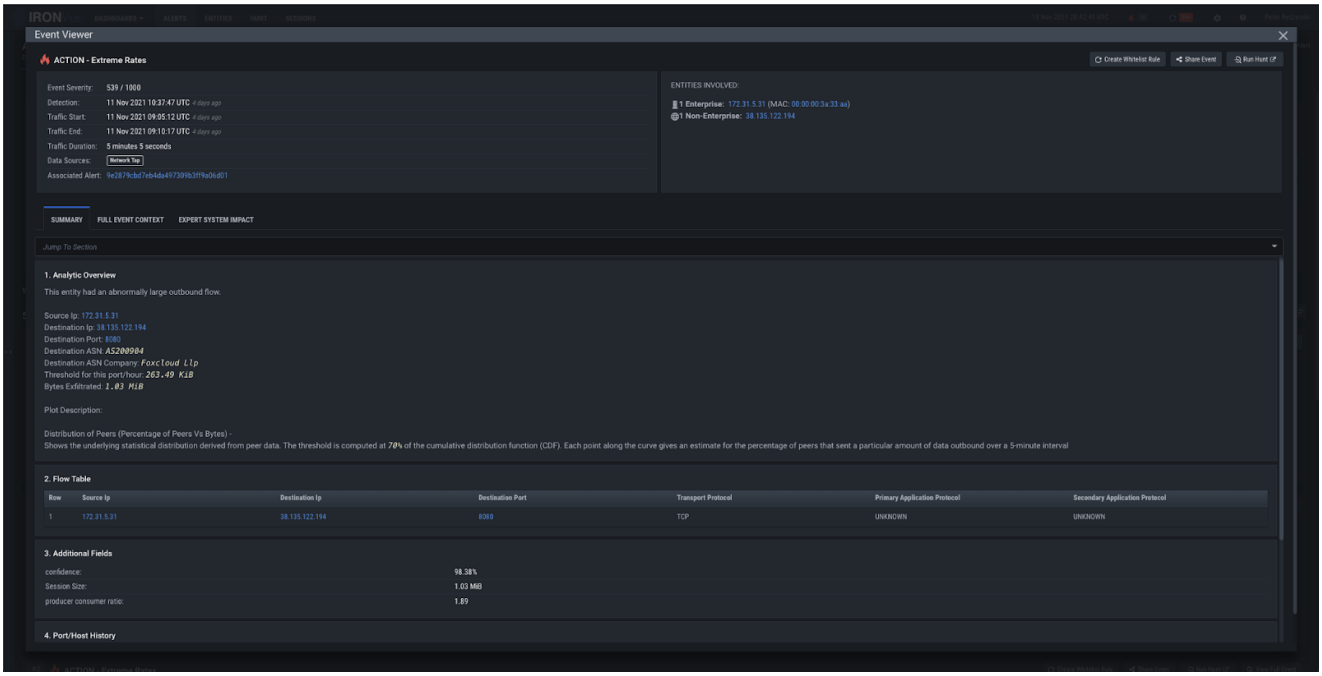
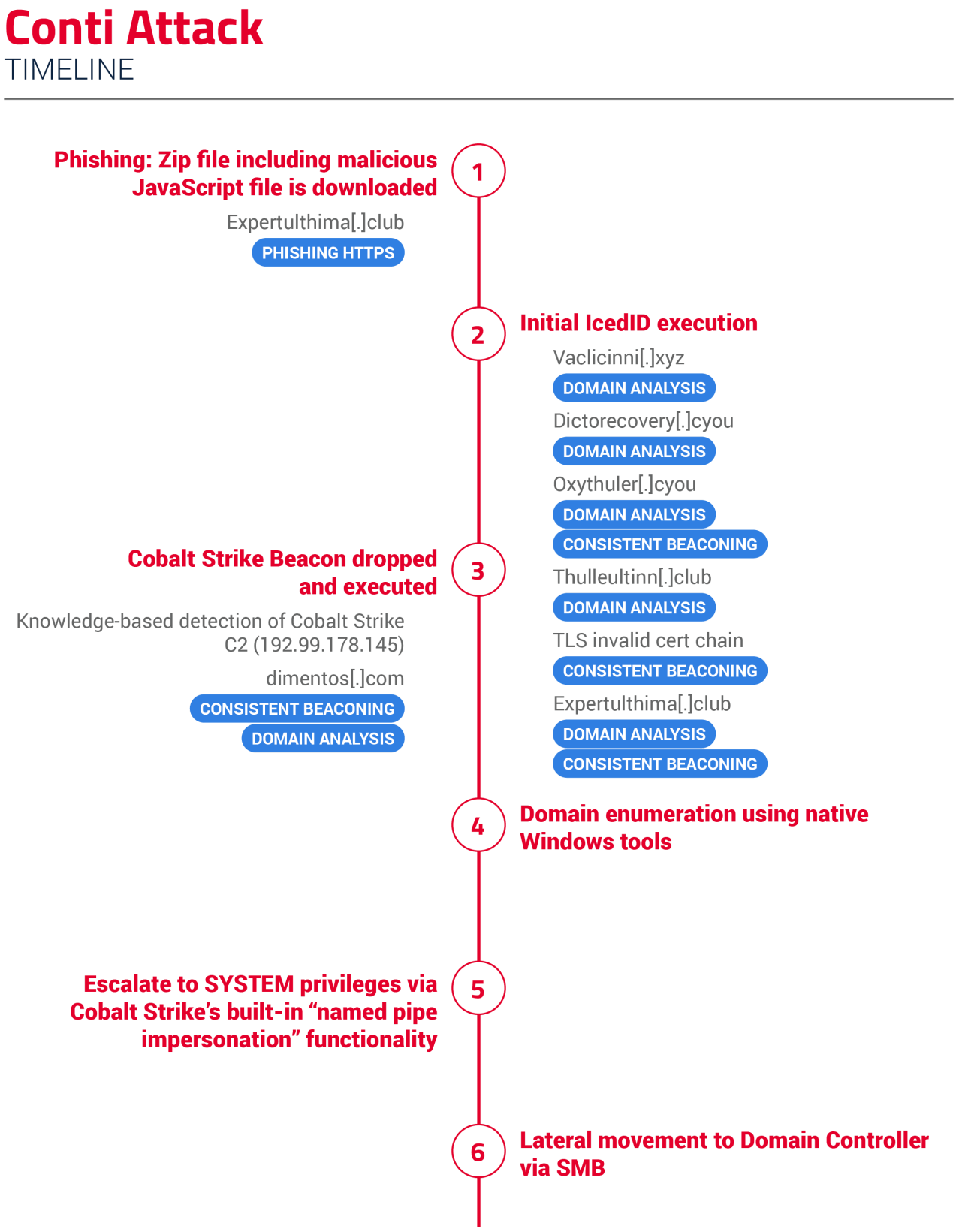
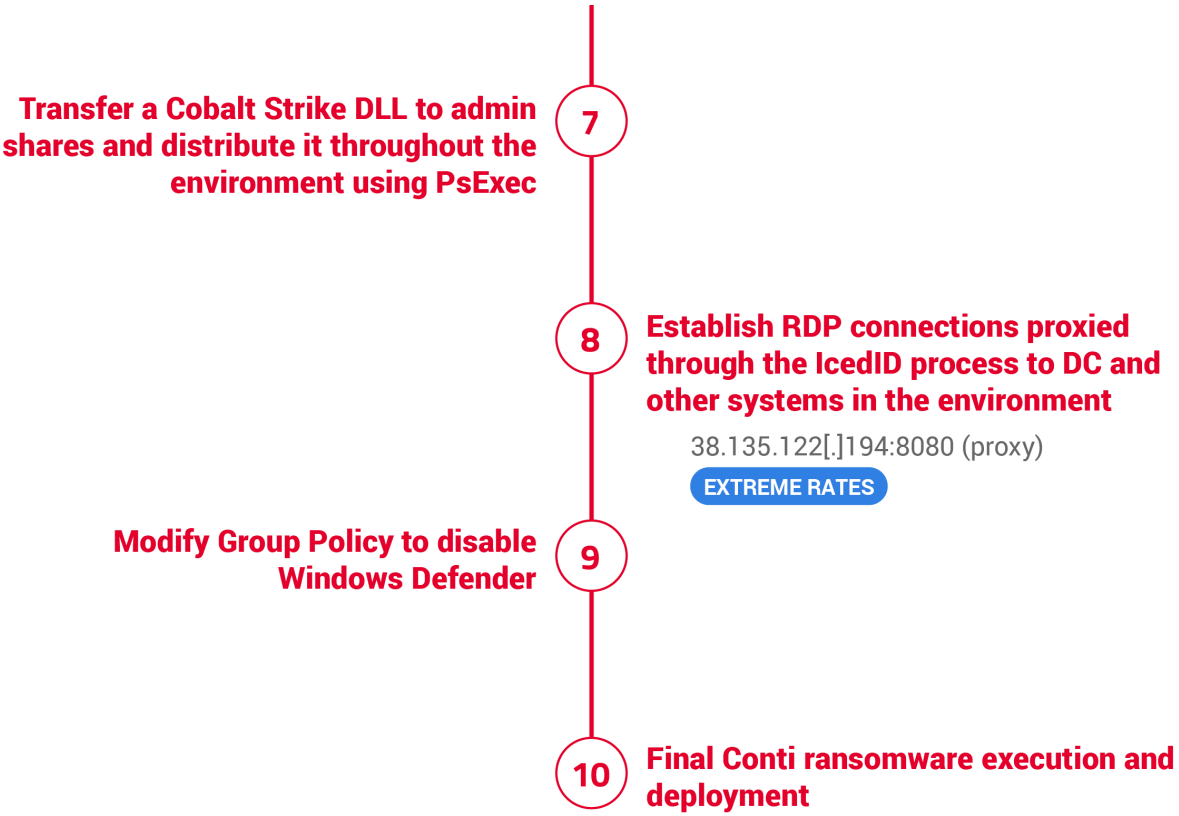


Figure 20: Extreme Rates analytic firing on 38.135.122.194

For defense evasion, the threat actors modified the Group Policy to disable Windows Defender and force updated it to all clients using Cobalt Strike. Around two and a half hours after initial intrusion, the Cobalt Strike Beacon processes inject the Conti DLL into memory, and all active systems are encrypted.





So what?

In this article, we explained how IronNet advanced analytics detect ransomware attacks by two of the most prolific ransomware groups: REvil and Conti. Despite the evasive strategies employed by both of these two threat groups, it is clearly apparent that through behavioral analytics, their behaviors are detectable across all stages of the kill chain and before a ransomware payload is ever executed.

About Ironnet

Founded in 2014 by GEN (Ret.) Keith Alexander, IronNet, Inc. (NYSE: IRNT) is a global cybersecurity leader that is transforming how organizations secure their networks by delivering the first-ever Collective Defense platform operating at scale. Employing a number of former NSA cybersecurity operators with offensive and defensive cyber experience, IronNet integrates deep tradecraft knowledge into its industry-leading products to solve the most challenging cyber problems facing the world today.

Back to IronNet Blog