# How IronNet's Behavioral Analytics Detect REvil and Conti Ransomware

ironnet.com/blog/ransomware-graphic-blog



Back to IronNet Blog <u>Threat Research</u> 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 <u>DFIR Report</u> published two separate articles outlining ransomware attacks by Conti and REvil, both of which leveraged the <u>lcedID trojan</u> 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 <u>REvil</u> 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 <u>Kaseya</u> and <u>JBS</u> Foods. Operating under a ransomware-as-a-service (RaaS) model, REvil was <u>ranked first</u> among the most common ransomware variants in the first half of 2021 with 14.2% of the total market share. In October 2021, REvil <u>reportedly</u> shut down its operations following the arrest of several of its members and the hijacking of its infrastructure by law enforcement.

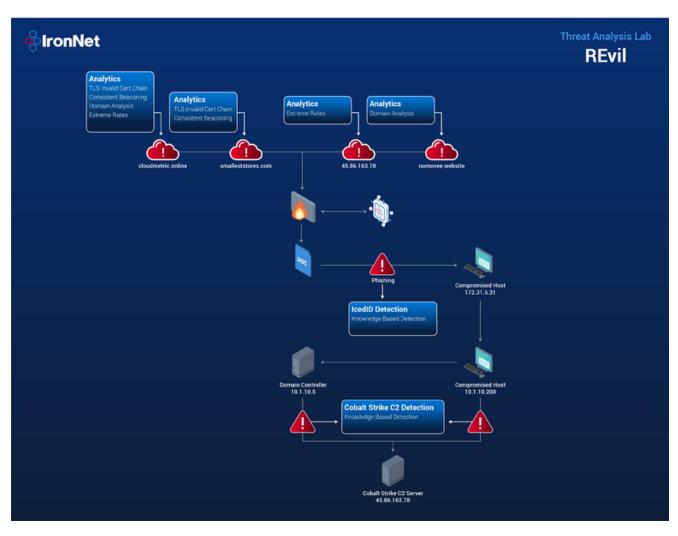


Figure 1: REvil malicious traffic and IronNet behavioral analytics

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.

IRONVUE DASHBOARDS -	ALERTS ENTITIES HUNT	SESSIONS		28 Oct 2021	18:47:39 UTC 🌲 👀 🔿 📴 💠 \varTheta Peter Rydzynski
Sort by: Enterprise Alert Score → ↓7	C2 - Consistent Beaconin Detection: 6 Oct 2021 00:55:58 UTC	g TLS Last Event: 6 Oct 2021 00:55:58 UTC   Alert Status: 🏴 Under Revie	w – Cancel Review – Close Alert   Analyst Rating: Unrated – Rat		
□•	OVERVIEW ACTIVITY IROND				
C2: Consistent Reacons(115 899     10est     10est     Detection 6 0ct 3221 005558 UTC     Last Foest 6 0ct 3221 005558 UTC     This Alert * * * * * * 1 №     Enterprise     Communities * * * * 1 №	Enterprise Alert Score B99 Enterprise Alert Score	At a Glance Event Discovered: 1 Event Data Sources: IntroDome Match Match Sequence: Enterprise Correlation Context: Domain IntroDome Commit: 0 main	MITRE ATTRCK Tactic: COMMAND AND CONTROLTA011 Technique: APPLICATION LAYER PROTOCOLT1071 0 Tactimique: EXPERTANTION TA010 Technique: EXPERTANTION OVER C2 CHANNELT1041 0	Targeted Techniques and Malware Families The Periodic Beaconing TLS (Transport Layer Security) analytic identifies when entities generate HTTPS/TLS activity consistent with repetitive attempts by malware to establish communications with a command and control server. Beaconing activity may indicate the presence of malware attempting to call home. Beaconing is used by a wide variety of malware, with examples including the Emissary trigon. ADVSTORESHLL, loylogger, Neuros bot,	Alert Aggregation Criteria
	Whitelisted Events: O Excluded 1 Event (5 Oct 2021 17:01:47 UTC	f 😧 💿 Included 🔿 Whitelisted Only 🚱			Sort Events by: Event Seventy • 47
	🕴 🤚 C2 - Consistent Bea	aconing TLS			
	Traffic Start: 5 Oct 2021 1			ntmes novouveo: <b>1 Enterprise:</b> 172.31.531 (MAC: 00.0030/38.333aa)	
1 - 1 of 1					

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

It is from here that IcedID pulls down Cobalt Strike Beacons from two different commandand-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.

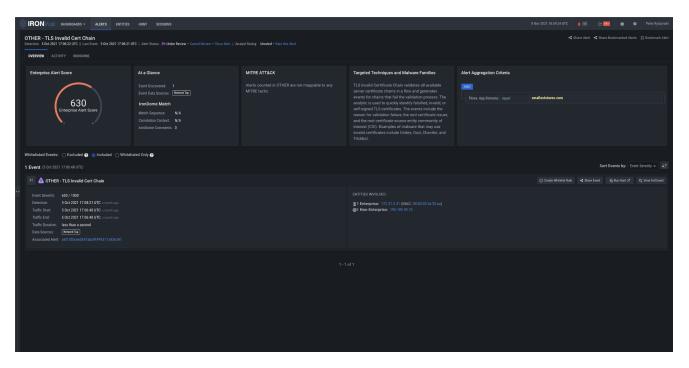


Figure 3: TLS Invalid Cert Chain analytic firing on smalleststores[.]com

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.

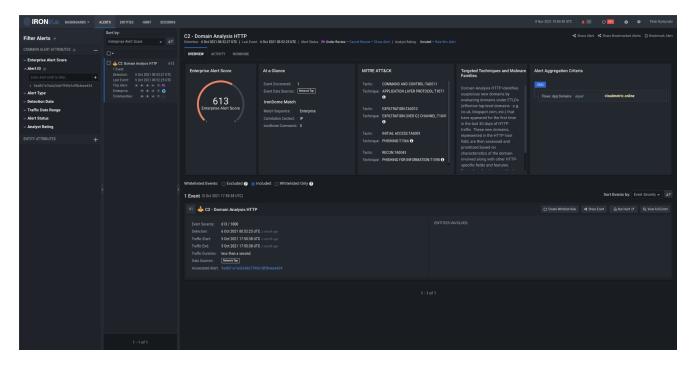


Figure 4: Domain Analysis HTTP analytic firing on cloudmetric[.]online

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.

IRONVUE DASHBOARDS - AL	LERTS ENTITIES HUNT SESSIONS					8 Nov 2021 19:04:01 UTC 🌲 50	C 📴 🌣 🛛 Peter Rydzynski
Filter Alerts * COMMON ALERT ATTRIBUTES * _	Sort by: Enterprise Alert Score - 47	C2 - Consistent Beaconing TLS Detection: 6 Oct 2021 08:56:00 UTC   Last Event OVERVIEW ACTIVITY IRONDOME	: 6 Oct 2021 00:55:59 UTC   Alert Status: 🏴 Under Raview – Can	cel Review – Close Alert   Analyst Rating: Unrated – Ra		< Share Alert 🔸	
- Enterprise Adert Score A Alert 10 vs  Tour Adert 10 vs  Adert 10 vs  Adert 10 vs  Adert 20 vs	C and a consistent beacourage 11.5 611     Serie     Detection 6.01 202 105:03:00.01C     Last Cevet 5.00.212 105:03:01C     This Aut *** *** ***     Exercise     Connectative     * *******     Connectative     * *******     Connectative	Enterprise Alert Score	At a Glance Event Discovered: I Event Dis Sources: EventData Event	MITRE ATTACK Tactic COMMAND AND CONTROL-TAROTT Technique APPLICATION LANCER PRODOCCT Technique DISTUTIATION FORMER O	071  The Periodic Beaconing TLS (Transport Layer Security) analytic identifies when entities generate HTTPS/TLS activity	Alert Aggregation Criteria	ebudmetric calina
		Whitelisted Events: O Excluded () () 1 Event (5 Oct 2021 17:07:54 UTC)	Included 🔿 Whitelisted Only 🍞				Sort Events by: Event Severity - 47
		💷 📥 C2 - Consistent Beaconing	TLS				
		Event Sevenity:         611 / 1000           Detection:         6 Oct 2021 00:558 07           Traffic Start:         SOct 2021 10:03:42 07           Traffic End:         5 Oct 2021 20:03:42 07           Traffic Start:         Soct 2021 20:03:42 07           Traffic Start:         Soct 2021 20:03:42 07           Traffic Start:         Shoars Starting St	C a month ago TC a month ago seconds		нтпез кичосиев. 1 Епterprise: 172.31.5.31 (MAC: 00.00.00.38.33.ав)		
	1 - 1 of 1						

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

						4 50 C 50		Peter Rydzynski
C2 - Consistent Beaconing TLS								
Detection: 6 Oct 2021 00:56:07 UTC   Last Event: 6 Oct 2021 00:56:02	UTC   Alert Status: 🏴 Under Review – Cancel Review – Close Alert   A	nalyst Rating: Unrated – Rate this Alert						
OVERVIEW ACTIVITY IRONDOME								
Enterprise Alert Score	At a Glance	MITRE ATT&CK	Targeted Techniques and Malware Families	Alert Aggregation Criteria				
	Events Discovered: 3	Tactic: COMMAND AND CONTROL:TA0011 Technique: APPLICATION LAYER PROTOCOL:T1071	The Periodic Beaconing TLS (Transport Layer Security) analytic identifies when entities generate	AND				
	Event Data Sources: Network Tap	Technique: APPLICATION LAYER PROTOCOL: 11071			smalleststores.com			
899	IronDome Match	Tactic: EXFILTRATION:TA0010	attempts by malware to establish communications with a command and control server. Beaconing					
Enterprise Alert Score	Match Sequence: Enterprise	Technique: EXFILTRATION OVER C2 CHANNEL: T1041 ()						
			attempting to call home. Beaconing is used by a wide variety of malware, with examples including the					
			Emissary trojan, ADVSTORESHELL keylogger, Necurs					
Whitelisted Events:      Excluded      O     Included      White	Histed Only 2							
						Sort	wante hur Eus	nt Severity 👻 🐙
3 Events (5 Oct 2021 17:06:45 UTC To 5 Oct 2021 18:05:02 UTC)							irento by. cite	
🕴 📥 C2 - Consistent Beaconing TLS								
Event Severity: 899 / 1000								
Detection: 6 Oct 2021 00:56:00 UTC a month ago								
Traffic End: 5 Oet 2021 20:05:53 UTC a month ago								
Traffic Duration: 2 hours 51 seconds								
Data Sources: Retwork Tap Associated Alert: d886e3Sce2fd4d82bc87918f69455f46								
#2 📥 C2 - Consistent Beaconing TLS								
Event Severity: 899 / 1000								
Traffic End: 5 Oct 2021 20:01:18 UTC a month ago								
Traffic Duration: 2 hours 11 minutes 35 seconds								
Data Sources: Network Tap Associated Alert: d886e35ce2fd4d82bc87918f69455f46								
R3 👶 C2 - Consistent Beaconing TLS								

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).

IRONVUE DASHBOARDS - ALERTS						4 🗵 C 📴		
OTHER - Knowledge-Based Detection Detection: 5 Det 2021 17:25:16 UTC   Last Event: 5 Det 20 OVERVIEW ACTIVITY IRONDOME	21 1950:56 UTC   Alert Status:  Ni Under Review - Cancel Review - Close Alert	Analyst Rating: Unrated - Rate this Alert						
Enterprise Alert Score	At a Glance	MITRE ATT&CK	Targeted Techniques and Malware Families	Alert Aggregation Criteria				
	Events Discovered: 114 Event Data Sources: Metwork Tap	Alerts counted in OTHER are not mappable to any MITRE tactic.	Knowledge-Based Detection is designed to catch threats in real time at the sensor. These rules typically	AND				
900	IronDome Match		focus on deep packet inspection (content based signatures).		ET MALWARE Cobalt S	trike Malleable C2 .	JQuery Custom I	Profile M2
Enterprise Alert Score					Malware Command an	d Control Activity D	etected	
	Correlation Context: N/A IronDome Comments: 0				2033658			
Whitelisted Events: O Excluded ?  Included	○ Whitelisted Only ?							
114 Events (5 Oct 2021 17:24:24 UTC To 5 Oct 2021						Sort E	vents by: Eve	
#1 A Risk Event: OTHER - Knowledge-Based Detection	'n						🧕 Run Hunt (2	
Detection: 5 Oct 2021 17:59:24 UTC a month     Traffic Start: 5 Oct 2021 17:58:31 UTC a month			@2 Non-Enterprise: 45.86.163.78, 10.1.10.200					
Traffic Duration: less than a second Data Sources: Network Tap								
Associated Alert: f313a6d2c4e04ec4abb83bc8ba5								
#2 A Risk Event: OTHER - Knowledge-Based Detection	n							
			@2 Non-Enterprise: 45.86.163.78, 10.1.10.200					
Traffic Start: 5 Oct 2021 18:04:25 UTC a month Traffic End: 5 Oct 2021 18:04:25 UTC a month								
Traffic Duration: less than a second								
Disk Event:								
Risk Event: OTHER - Knowledge-Based Detection	'n						Q Run Hunt (3*	
Event Severity: 900 / 1000								

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

ON VILE DASHROARDS - ALERTS ENTITIES HUNT SESSIONS vent Viewer		E Nov 2021 19 1 4.8 UTC 🔹 186 🖉 🚾 💩 O Prive
Risk Event:     OTHER - Knowledge-Based Detection		C Dirate Whitelist Rule Q View Thread Intelligence Rule ◀ Share Event Q Rus Hunt C
	@2 Non-Enterprise: 10.1.10.5, 45.86.163.7	
Traffic Start: 5 Oct 2021 17:50:02 UTC a month app		
Traffic End: 5 Oct 2021 17:50:02 UTC a month app		
Traffic Duration: less than a second		
SUMMARY FULL EVENT CONTEXT EXPERT SYSTEM IMPACT		
	UNKNOWN	
	2033658	
	Mahware Command and Control Activity Detected	
	ET MALWARE Cobalt Strike Malleable C2 JQuery Custom Profile M2	

*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.

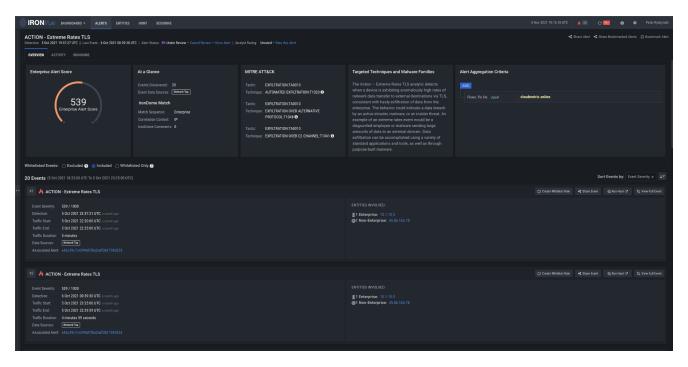
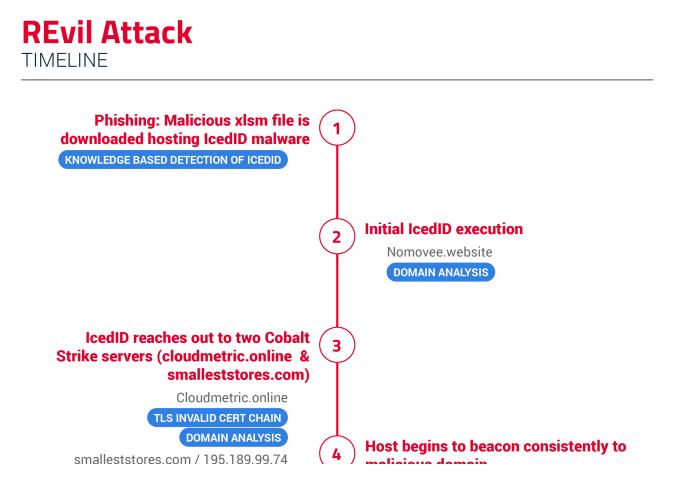
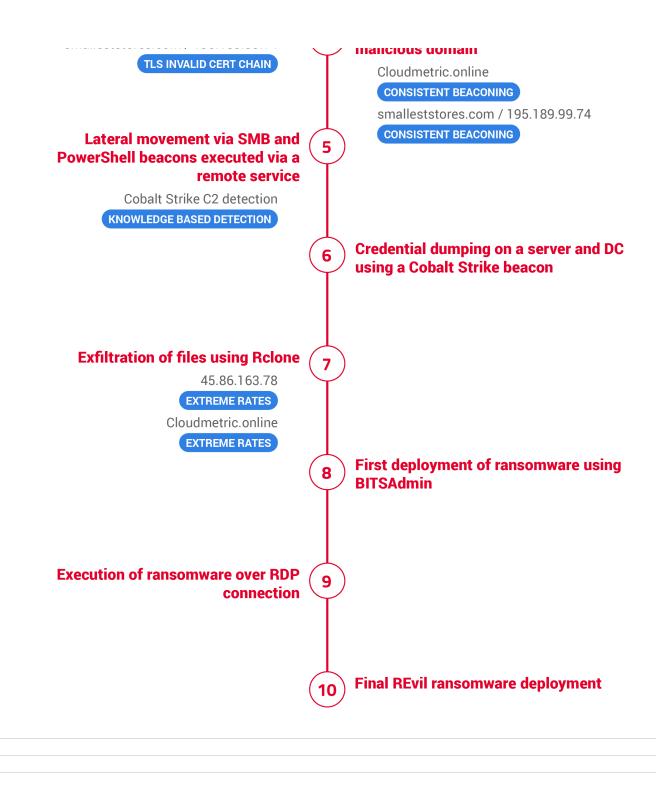


Figure 9: Extreme Rates TLS analytic firing on cloudmetric[.]online

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 <u>Conti</u>, 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.

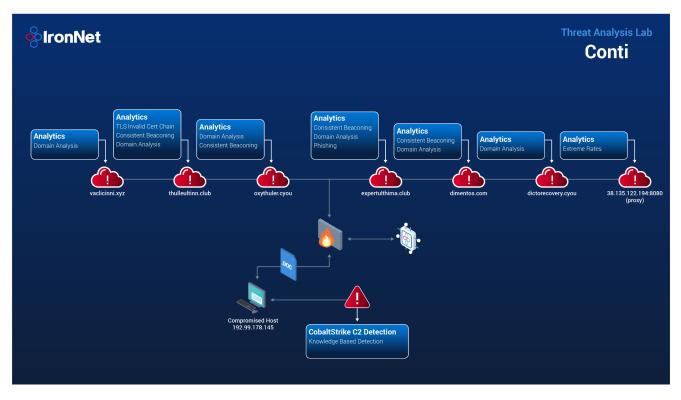


Figure 10: Conti malicious traffic and IronNet behavioral analytics

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.

Event Viewer					
	803 / 1000				
			@1 Non-Enterprise: 83.97.20.160		
	7 Oct 2021 10:59:35 UTC a month age				
SUMMARY P	FULL EVENT CONTEXT EXPERT SYSTEM IMPACT				
1. Analytic Over	erview				
			0-07.		
Read on Ironhi	Not's analysis this domain may be associated with phickle	na maluura or othar ausoiainua activitu			
2. Machine Lean	aming Risk Scores	Inpet Value(s)		Approximate Risk Score	
2. Machine Lean	arning Risk Scores				
2. Machine Lean Row Descrip 1 FQDN	arning Risk Scores eription N				
2. Machine Lean Row Descrip 1 FQDN 2 Overall	enning Risk Scores orgeten Ri zall Behaver				
2. Machine Learn Row Descrip 1 FQDN 2 Overall 3. Suspicious Co	enning Risk Scores orgeten Ri zall Behaver				
2. Machine Lean     Row Descrip     1 FQDN     2 Overall     3. Suspicious Co     1.23	enning Risk Scores orgeten Ri zall Behaver				
2. Machine Lean Row Descrip 1 FQDN 2 Overall 3. Suspicious Co	enning Risk Scores orgeten Ri zall Behaver				
2. Machine Lean Row Descrip 1 FCIDN 2 Overall 3. Suspicious Ce 123 100 0.21	enning Risk Scores orgeten Ri zall Behaver				
2. Machine Lean Row Descrip 1 FODN 2 Overall 3. Suspicious Co 123 103 0,21 0,51	enning Risk Scores orgeten Ri zall Behaver				
2. Machine Lean Row Descrip 1 FQDN 2 Overall 3. Suspicious Co	ening Risk Scores erigiens eri				
2. Machine Lean Row Descrip 1 FQDN 2 Overall 3. Suspicious Co	ening Risk Scores erigiens eri				
2. Machine Lean Row Descrip 1 FQDN 2 Overall 3. Suspicious Co	ening Risk Scores erigiens eri				
2. Machine Lean Row Descrip 1 FQDN 2 Overall 3. Suspicious Co	ening Risk Scores erigiens eri				

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.

IRONVue dashboards - Alerts entities	HUNT SESSIONS				8 Nov 2021 19:20:39 UTC 💧 💷 📿	: 💯 💠 🛛 Peter Rydzynski
C2 - Domain Analysis HTTP Detection: 4 Oct 2021 00:52:55 UTC   Last Event: 4 Oct 2021 00:52:24 OVERVIEW ACTIVITY IRONDOME	UTC   Alert Status:  Ni Under Review - Cancel Review - Close Alert   An	alyst Rating: Unrated - Rate this Alert				hare Bookmarked Alerts 🔲 Bookmark Alert
Enterprise Alert Score 637 Enterprise Alert Score	At a Glance Event Bulk sources: Event Bulk sources: Event Bulk sources: Event Bulk Sources: NA Source Bulk Bulk Bulk Source Bulk Bulk Bulk Source Bulk Bulk Source Bul	MITEE ATTACK           Tacin:         COMMAND AND CONTROL TACHT           Technique:         APPLICATION LANDER MOLTOCOLLTION OF           Technique:         DIRTRATION ANDRE CONTROL TACHT OF           Technique:         DIRTRATION ANDRE CONTROL TACHT OF           Technique:         DIRTRATION ANDRE CONTROL TACHT OF           Technique:         PRESIMENT TASK OF           Technique:         RESIMENT TASK OF           Technique:         RECONTRADOR	Targetci Techniques and Malware Families Commit Analysis (TTP) identifies suspicions are observed to the suspicion of the suspicion of the (iffective top prime domains - rg do call, biogenetic com, etc.) that have separated for the first men in the tail 30 good of UTP Telfact. These new domains, represented in the TTP host field, are then assessed and protection based on Analysis and the domain models along with other ITTP-specific that along atTP-based instants. The analysis that along atTP-based instants are and that along atTP-based instants days and the domain models along with top attributes that the along atTP-based instants days and the along atTP-based instants days and the along attributes and the along atTP-based instants days and the along attributes and the along attributes attributes and the along attributes attributes at the along attributes attributes attributes att	Alert Aggregation Criteria	weeksioni aya	
Whitelisted Events: Excluded () included () White 1 Event (5 oct 2021 18:7281 UTC) 1 @ C2 - Domain Analysis HTTP	listed Only					Sort Events by: Event Severity + 47 -Q Rue Hurt Lt Q, View Full Event
Event Sevenity         437 / 1000           Celection:         6 Oct 2001 00 52:23 UTC smooth age           Traffic Dart:         5 Oct 2001 10:27 UTC smooth age           Traffic Dart:         5 Oct 2001 11:27 UTC smooth age           Traffic Dart:         5 Oct 2001 11:27 UTC smooth age           Traffic Dart:         In the avened           Data Score:         Second 2001 11:27 Second 2000           Associated Alert:         Second 2007/42/25/04/75/201 44605 MMMd			ылттіів ничилію. <b>11 благрана:</b> 17231.531 (МАС: 08.00.003433 ац)			
		1-1	of1			

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.

IRONVUE DASHBOARDS - ALERTS ENTITIES	S HUNT SESSIONS				15 Nov 2021 15:54:56 UTC	4 10 C	•	Peter Rydzynski
C2 - Consistent Beaconing TLS Detection: 12 Nov 2021 00:56:13 UTC   Last Event: 12 Nov 2021 17:5	1:24 UTC   Alert Status: 🏴 Awaiting Review – Open for Review   Analys	t Rating: Unnated - Rate this Alert						
OVERVIEW ACTIVITY IRONDOME								
Enterprise Alert Score	At a Glance Events Discovered: 2	MITRE ATT&CK	Targeted Techniques and Malware Families The Periodic Beaconing TLS (Transport Layer	Alert Aggregation Criteria				
899 Enterprise Alert Score	Event Data Sources. (Www.Yay) HordDome Match Match Sequence: Enterprise Correlation Contact: Domain, (P IreaDome Comments: 0	Technique: APPLICATION LAVERPROTOCOL.TIOT O Technique: DRIETRATION TMOTIO Technique: EXPECTRATION OVER C2 CHANNEL.TION O	Security) analytic identifies when entitles generate HTTPs/TL socities when integration in the period attempts by malware to establish communications with a command and control evence. Becoming activity may indicate the presence of malware attempting to active home. Becoming is used by a wide variety of malware, with examples including the Emissary traina. DAYSTORESHELL keylogger, Nexura bot, and CozyGar RAT.		orythuler.cyou			
Whitelisted Events:         Excluded         Included         Whitelisted         Whitelisted <thwitelisted< th="">         Whitelisted</thwitelisted<>						Sort E	ents by: Event	
1 6 C2 - Consistent Beaconing TLS								
Event Severity: 894/1000     Event Severity: 12 Nov 2011 75:124 UTC 2 core part     Testlis Event 11 Nov 2021 15:843 UTC 2 core part     Testlis Event 11 Nov 2021 15:843 UTC 2 core part     Testlis Event 11 Nov 2021 15:843 UTC 4 core part     Testlis Event 11 Nov 2021 15:843 UTC 4 core part     Testlis Event 11 Nov 2021 15:843 UTC 4 core part     Testlis Event 11 Nov 2021 15:843 UTC 4 core part     Testlis Event 11 Nov 2021 15:843 UTC 4 core part     Testlis Event 11 Nov 2021 15:843 UTC 4 core part     Testlis Event 11 Nov 2021 15:843 UTC 4 core part     Testlis Event 11 Nov 2021 15:843 UTC 4 core part     Testlis Event 11 Nov 2021 15:843 UTC 4 core part     Testlis Event 11 Nov 2021 15:843 UTC 4 core part     Testlis Event 11 Nov 2021 15:843 UTC 4 core part     Testlis Event 11 Nov 2021 15:843 UTC 4 core part     Testlis Event 11 Nov 2021 15:843 UTC 4 core part     Testlis Event 11 Nov 2021 15:843 UTC 4 core part     Testlis Event 11 Nov 2021 15:843 UTC 4 core part     Testlis Event 11 Nov 2021 15:843 UTC 4 core part     Testlis Event 11 Nov 2021 15:843 UTC 4 core part     Testlis Event 11 Nov 2021 15:843 UTC 4 core part     Testlis Event 11 Nov 2021 15:843 UTC 4 core part     Testlis Event 11 Nov 2021 15:845 UTC 4 core part     Testlis Event 11 Nov 2021 15:845 UTC 4 core part     Testlis Event 11 Nov 2021 15:845 UTC 4 core part     Testlis Event 11 Nov 2021 15:845 UTC 4 core part     Testlis Event 11 Nov 2021 15:845 UTC 4 core part     Testlis Event 11 Nov 2021 15:845 UTC 4 core part     Testlis Event 11 Nov 2021 15:845 UTC 4 core part     Testlis Event 11 Nov 2021 15:845 UTC 4 core part     Testlis Event 11 Nov 2021 15:845 UTC 4 core part     Testlis Event 11 Nov 2021 15:845 UTC 4 core part     Testlis Event 11 Nov 2021 15:845 UTC 4 core part     Testlis Event 11 Nov 2021 15:845 UTC 4 core part     Testlis Event 11 Nov 2021 15:845 UTC 4 core part     Testlis Event 11 Nov 2021 15:845 UTC 4 core part     Testlis Event 11 Nov 2021 15:845 UTC 4 core part     Testlis Event 11 Nov 2021 15:845 UTC 4 core part			ENTITIE RODUED:					
🕫 📥 C2 - Consistent Beaconing TLS								
Event Severity:         699 / 1000           Detectors:         12 No.2011 05 46:13 UTC # days age           Trafic Exert:         13 No.2011 15:82:83 UTC # days age           Trafic Exert:         11 No.2011 15:84.9 UTC # days age           Trafic Exert:         1 No.2011 15:84.9 UTC # days age           Trafic Exert:         1 No.2011 15:84.9 UTC # days age           Traffic Exert:         1 No.2011 15:84.9 UTC # days age           Traffic Exert:         1 No.2011 15:84.9 UTC # days age           Associated Alert:         2 Associated Alert:			ENTITES INVOLUES:					

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

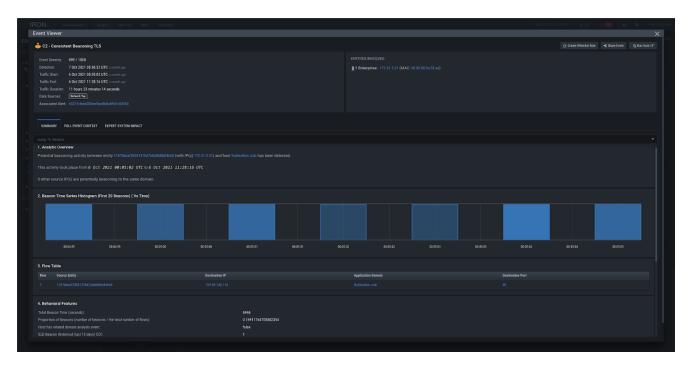


Figure 14: Consistent Beaconing TLS analytic firing on thulleultinn[.]club

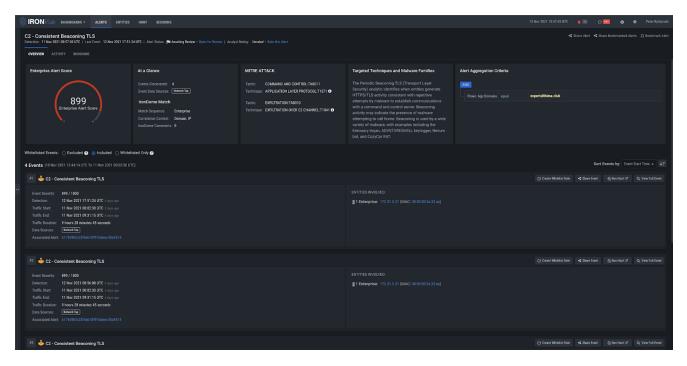


Figure 15: Consistent Beaconing TLS analytic firing on expertulthima[.]club

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.

IRON/UE DASHBOARDS - ALERTS ENTITIES	HUNT SESSIONS				8 Nov 2021 19:18:41 UTC 🔺 📧 C: 🏧 🏚 Peter Rydzynski
OTHER - TLS Invalid Cert Chain           Detection:         5 Oct 2021 18:19:14 UTC   Last Event:         5 Oct 2021 18:19:13 U           OVERVIEW         ACTIVITY         IRONDOME	ΠC   Alert Status: <b>Piu Under Review -</b> Carcel Review - Close Alert   Ani	Ayst Rating: Unrated - Rate this Alert			< Share Alert < Share Bookmarked Alert 🔲 Bookmark Alert
Enterprise Alert Score	At a Glance	MITRE ATT&CK	Targeted Techniques and Malware Families	Alert Aggregation Criteria	
		Alerts counted in OTHER are not mappable to any MITRE tactic.	TLS Invalid Certificate Chain validates all available server certificate chains in a flow and generates	AND	
560	Event Data Sources: (Network Tap)		events for chains that fail the validation process. The analytic is used to quickly identify falsified, invalid, or		oxythuler.cyou
Enterprise Alert Score	Match Sequence: N/A Correlation Context: N/A		self-signed TLS certificates. The events include the reason for validation failure, the root certificate issuer, and the root certificate source entity community of		
- x'			interest (COI). Examples of malware that may use invalid certificates include Dridex, Gozi, Chanitor, and Trickbot.		
Whitelisted Events: O Excluded 🚱 💿 Included O Whiteli	isted Only 🕤				
1 Event (5 Oct 2021 18:17:40 UTC)					Sort Events by: Event Sevenity - 47
#1 🛕 OTHER - TLS Invalid Cert Chain					C <sup>a</sup> Create Whitelist Rule  < Share Event - 숏 Rus Hunt C <sup>a</sup> Q, View Full Event
Event Severity: 560 / 1000 Detection: 5 Oct 2021 18:19:12 UTC a month app			ENTITIES INVOLVED: 1 Enterprise: 172.31.5.31 (MAC: 00.00.00.3a.33.aa)		
Traffic Start: 5 Oct 2021 18:17:40 UTC a month ago Traffic End: 5 Oct 2021 18:17:40 UTC a month ago			T Enterprise: 172.31(MAC: 00.000038:33.83)     T Non-Enterprise: 159.89.140.116		
Traffic Duration: less than a second Data Sources: Retwork Tap					
Associated Alert: 026b135d510a4d8e98154a72919cb257					

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).

IRONVUE DASHBOARDS - ALERTS ENTITLE	s hunt sessions			15 Nev 2021 20:37:19 UTC 💧 📧 C 💴 🌣 🛛 Peter Rydzynski
	2223 UTC   Alert Status: Ps Under Review - Cascel Review - Close Alert	Analyst Rating: Unrated - Rate this Alert		
OVERVIEW ACTIVITY IRONDOME				
Enterprise Alert Score	At a Glance	MITRE ATT&CK	Targeted Techniques and Malware Families	Alert Aggregation Criteria
	Events Discovered: 14	Alerts counted in OTHER are not mappable to any MITRE tactic.	Knowledge-Based Detection is designed to catch threats in real time at the sensor. These rules typically	AND
	Event Data Sources: Metwork Tag		focus on deep packet inspection (content based	Flows: Alert Signature Name equal ET MALWARE Cobalt Strike Maileable C2 Profile (btn_bg)
900	IronDome Match			
Enterprise Alert Score				Flows: Alert Category equal Malware Command and Control Activity Detected
				Flows: Alert Signature Id equal 2032964
Whitelisted Events: O Excluded ? • Included O Whit	relisted Only 🕑			
14 Events (11 Nov 2021 07:34:40 UTC To 11 Nov 2021 10:01:2				Sort Events by: Event Start Time + 47
#1 A Risk Event: OTHER - Knowledge-Based Detection				
Detection: 11 Nov 2021 10:02:23 UTC 4 days age			@2 Non-Enterprise: 172.31.5.31, 192.99.178.145	
Traffic Start: 11 Nov 2021 10:01:22 UTC & days ago				
Traffic End: 11 Nov 2021 10:01:22 UTC 4 clays ago Traffic Duration: less than a second				
Data Sources: Network Tap				
THER - Knowledge-Based Detection				
Event Severity: 900 / 1000				
Detection: 11 Nov 2021 10:00:48 UTC -/ clarst ago			@2 Non-Enterprise: 172.31.5.31, 192.99.178.145	
Traffic Start: 11 Nov 2021 09:59:52 UTC 4 days app			ar normalities transform, transformer	
Traffic End: 11 Nov 2021 09:59:52 UTC 4 days ago				
Traffic Duration: less than a second				
Data Sources: Network Tap				
Risk Event: OTHER - Knowledge-Based Detection				
Event Severity: 900 / 1000				

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

۲	IRONVUE DASHBOARDS - ALERTS ENTITIES	HUNT SESSIONS						•	
-	OTHER - Knowledge-Based Detection Detection: 11 Nov 2021 07:35:43 UTC   Last Event: 11 Nov 2021 16:02: OVERNEEN ACTIVITY IRONDOME	19 UTC   Alert Status: 🏴 Availing Review – Open for Review   Analyst	Rating: Unrated - Rate this Alert						
Γ	Enterprise Alert Score	At a Glance	MITRE ATT&CK	Targeted Techniques and Malware Families	Alert Aggregation Criteria				
			Alerts counted in OTHER are not mappable to any	Knowledge-Based Detection is designed to catch	AND				
				threats in real time at the sensor. These rules typically focus on deep packet inspection (content based	Flows: Alert Signature Name equal	ET MALWARE Cobait	t Strike Malleable (	C2 Profile (sessi	on_id Cookie)
	900 Enterprise Alert Score	IronDome Match			Flows: Alert Category equal	Malware Command a	and Control Activity	v Datacted	
		Match Sequence: N/A Correlation Context: N/A						Junio	
						2032965			
	Whitelisted Events:         Excluded         Included         Whitel           22 Events         (11 Nov 2021 07:34:40 UTC To 11 Nov 2021 10:01:22 1)         (11 Nov 2021 10:01:22 1)         (11 Nov 2021 10:01:22 1)						Sort I	Events by: Even	
	at A Risk Event: OTHER - Knowledge-Based Detection						< Share Event		Q, View Full Event
1	Detection: 11 Nov 2021 10:02:18 UTC 4 days ago Traffic Start: 11 Nov 2021 10:01:22 UTC 4 days ago			2 Non-Enterprise: 172.31.5.31, 192.99.178.145					
	Traffic End: 11 Nov 2021 10:01:22 UTC 4 days ago								
	Traffic Duration: less than a second								
	Data Sources: Retwork Tap Associated Alert: 0f6e75976ec9417e8bf1e7f47017978c								
	ASSOCIATED AREL: UIDE/39/0EC941/E0011E/14/01/9/8C								
Ш.									
	P2 A Risk Event: OTHER - Knowledge-Based Detection								
	Event Severity: 900 / 1000								
	Detection: 11 Nov 2021 10:02:08 UTC 4 days ago			@2 Non-Enterprise: 172.31.5.31, 192.99.178.145					
	Traffic Start: 11 Nov 2021 10:01:11 UTC 4 days ago								
	Traffic End: 11 Nov 2021 10:01:11 UTC 4 days app Traffic Duration: less than a second								
	Data Sources: NetworkTap								
	Associated Alert: 0f6e75976ec9417e8bf1e7f47017978c								
	Risk Event: OTHER - Knowledge-Based Detection								
	Event Severity: 900 / 1000								

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.

RON/UE dashboards - alerts chittles Event Viewer	HUNT SESSIONS								φ v ,
🕹 C2 - Consistent Beaconing HTTP								C Create Whitelist Rule	
Detection: 12 Nov 2021 10:48:43 UTC 3 days ago					1 Enter				
Traffic Start: 11 Nov 2021 07:33:43 UTC 5 days app									
Traffic End: 11 Nov 2021 12:00:14 UTC 4 days apo									
Traffic Duration: 4 hours 26 minutes 31 seconds									
SUMMARY FULL EVENT CONTEXT EXPERT SYSTEM IMPA									
1. Analytic Overview									
Potential beaconing activity between entity 1187bbeaf2004	137547e8ddfd8d14660 (with	(P(s) 172 31 5 31) and host d	Simentos com has been d	letected.					
This activity took place from 12 Nov 2021 07:33:43	UTC to 11 Nov 2021 1.	2:00:14 UTC							
with a beacon jitter of 0.048									
2. Beacon Time Series Histogram (First 20 Beacons) ( Vs	Time)								
3. Flow Table									
		Destination IP			Applicatio		estination Port		
4. Behavioral Features									
Total Beacon Time (seconds):			9216						
Proportion of Beacons (number of beacons / the total number of	flows):		0.803137254901960	08					

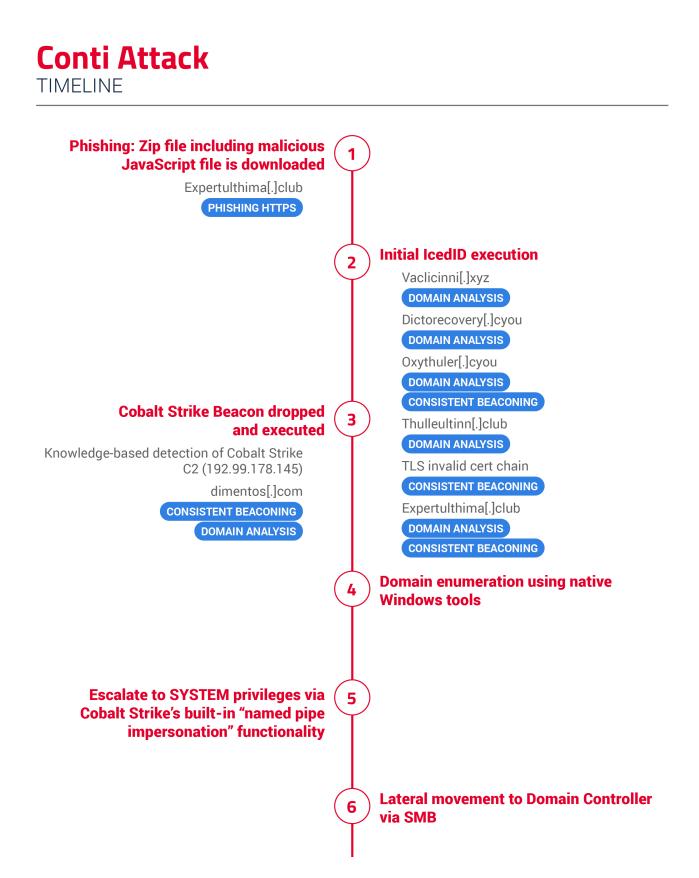
Figure 19: Consistent Beaconing HTTP analytic firing on dimentos[.]com

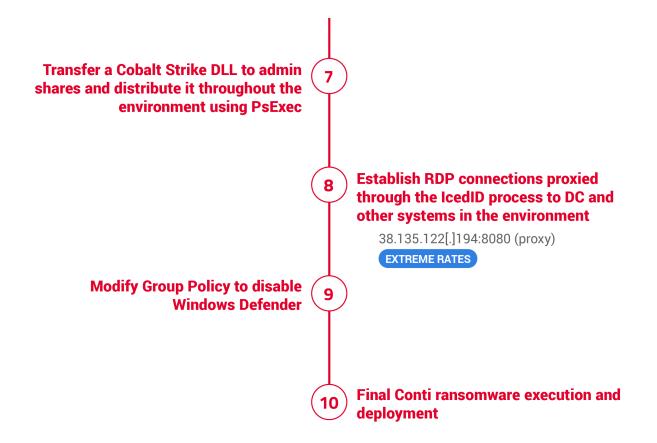
Later on, the attackers establish RDP connections to the DC and other systems throughout the environment. To do this, they use a redirector (38.135.122.194) to proxy the RDP traffic passing through the IcedID process. This activity was caught by our Extreme Rates analytic.

Event Viewer					
ACTION - Extreme Rates					
Event Severity: 539 / 1000					
Detection: 11 Nov 2021 10:37:47 UTC 4 days ag			1 Enterprise: 172.31.5.31 (MAC		
Traffic Start: 11 Nov 2021 09:05:12 UTC - days ap			@1 Non-Enterprise: 38.135.122.1		
Traffic End: 11 Nov 2021 09:10:17 UTC 4 days ag					
Traffic Duration: 5 minutes 5 seconds					
Data Sources: Metwork Tap					
SUMMARY FULL EVENT CONTEXT EXPERT SYST	TEM IMPACT				
1. Analytic Overview					
Destination Port: 8080 Destination ASN: AS200904					
Destination ASN Company: Foxcloud Llp					
Threshold for this port/hour: 263.49 KiB					
Distribution of Peers (Percentage of Peers Vs Byte Shows the underlying statistical distribution derive					
2. Flow Table					
				Primary Application Protocol	Secondary Application Protocol
3. Additional Fields					
		98.38%			
		1.03 MiB			
4. Port/Host History					

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