



**Ransomware Rebranding...
So Hot Right Now!**



Drew Schmitt

GRIT Lead Analyst

Who Am I?

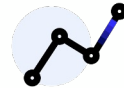
- 9+ years in Infosec
- Responsible for GRIT Operations and Threat Research
- Specialty: Malware Research
- Past lives in IT, SOC, DFIR

Agenda



A Brief History of Ransomware Rebranding

- 2020 – Present
- Rebranding Taxonomy
- Rebranding's effects on the Blue Team



Rebranding Case Studies

- Impacts of Rebranding on Operational Capacity
- Statistics based on Taxonomy



Tips and Tricks for Identifying Rebranding

- Code Level Analysis
- Behavioral Analysis/Threat Profiles
- Avoiding Pitfalls



Putting this Knowledge to Work

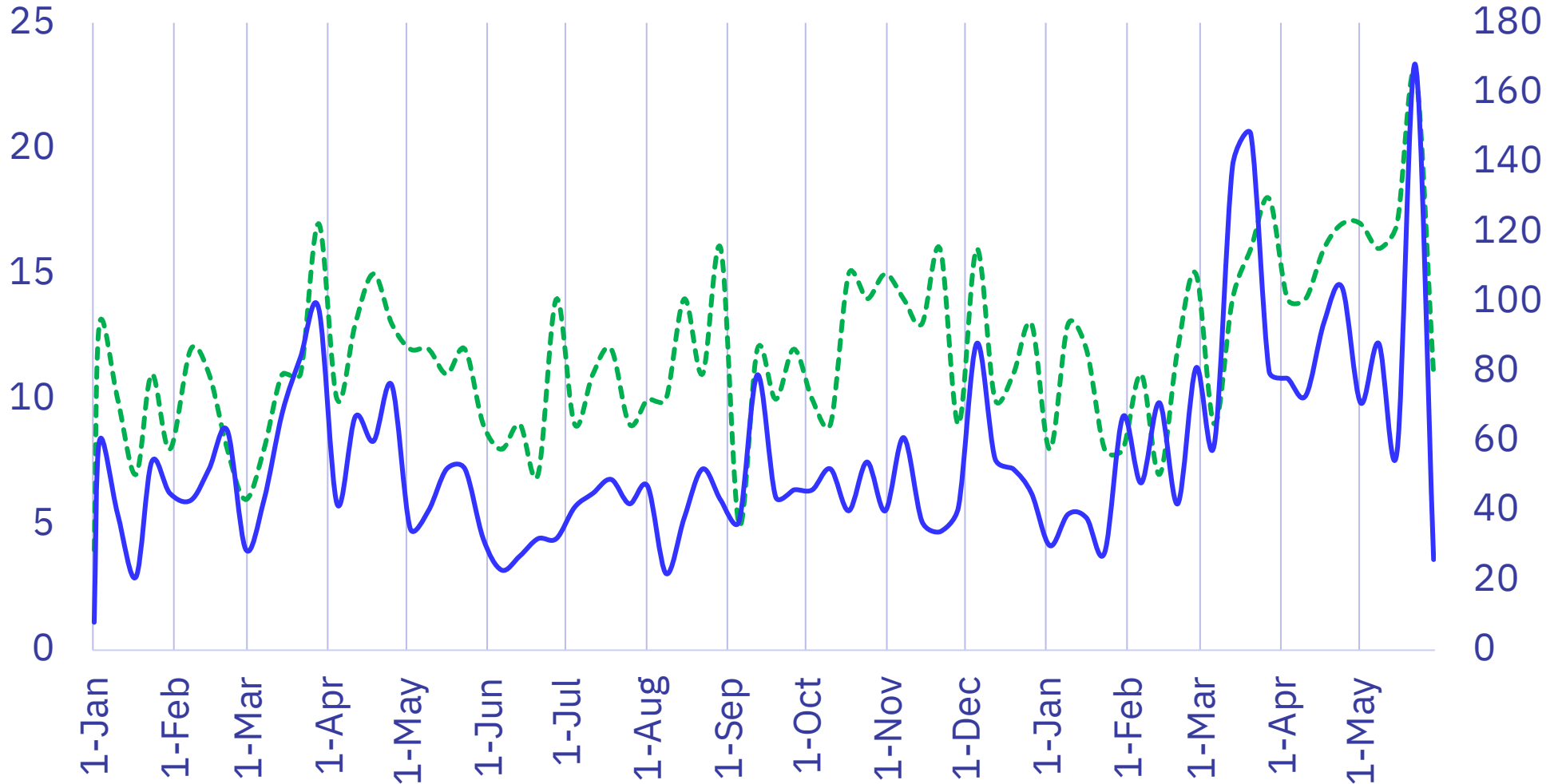
- Communicate the Intelligence
- Model the Intelligence, then Hunt it
- Call to Action: Intelligence Sharing for the Win!

RANSOMWARE REBRANDING



SO HOT RIGHT NOW

Rate of Publicly Posted Ransomware Victims (2022 - Present)



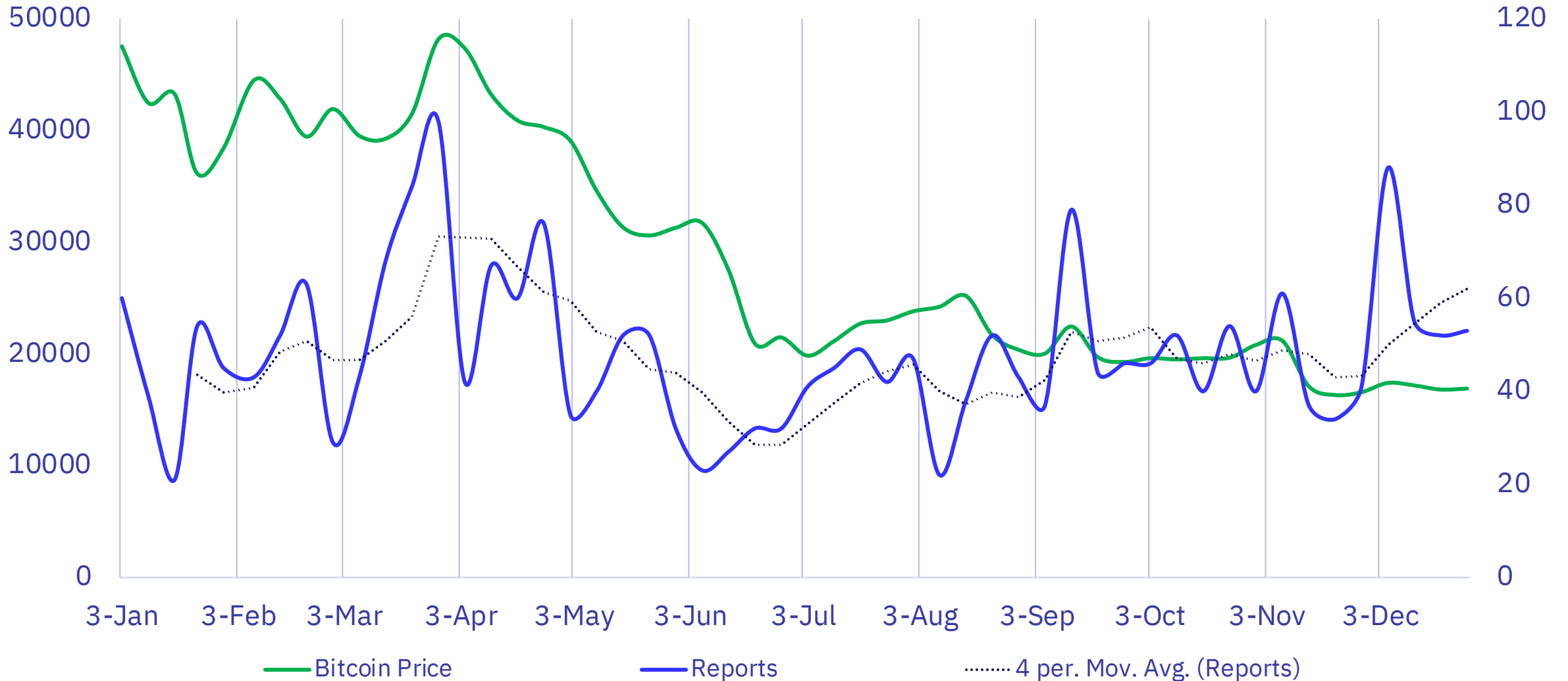
● Total Posts
4156

● Total Groups
71

Average Posts per Week
55.2 (48.1 in 2022)

Average Groups per Week
11.7 (11.2 in 2022)

Rate of Publicly Posted Ransomware Victims vs Price of Bitcoin (2022)



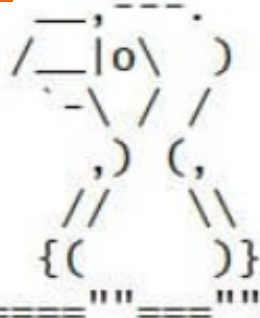
A Brief History of Ransomware Rebranding

REVIL

Defray777

Darkside

Black Basta



MACAW
LOCKER

EVIL CORP



Hive Ransomware



Egregor



AvosLocker

CONTI



payload.bin

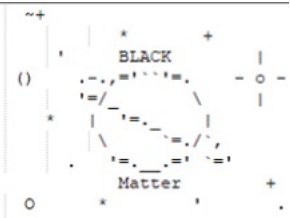
Grief



Hades
ransomware.



WastedLocker



Bitpaymer

BLACKHEAT



**MOUNT
LOCKER**

**GANDCRAB
RANSOMWARE**



PHOENIX CRYPTOLOCKER

RANSOMEXX



Maze Ransomware



A Taxonomy for Ransomware Rebranding

Splinter



Full-Time



Activity

Duration

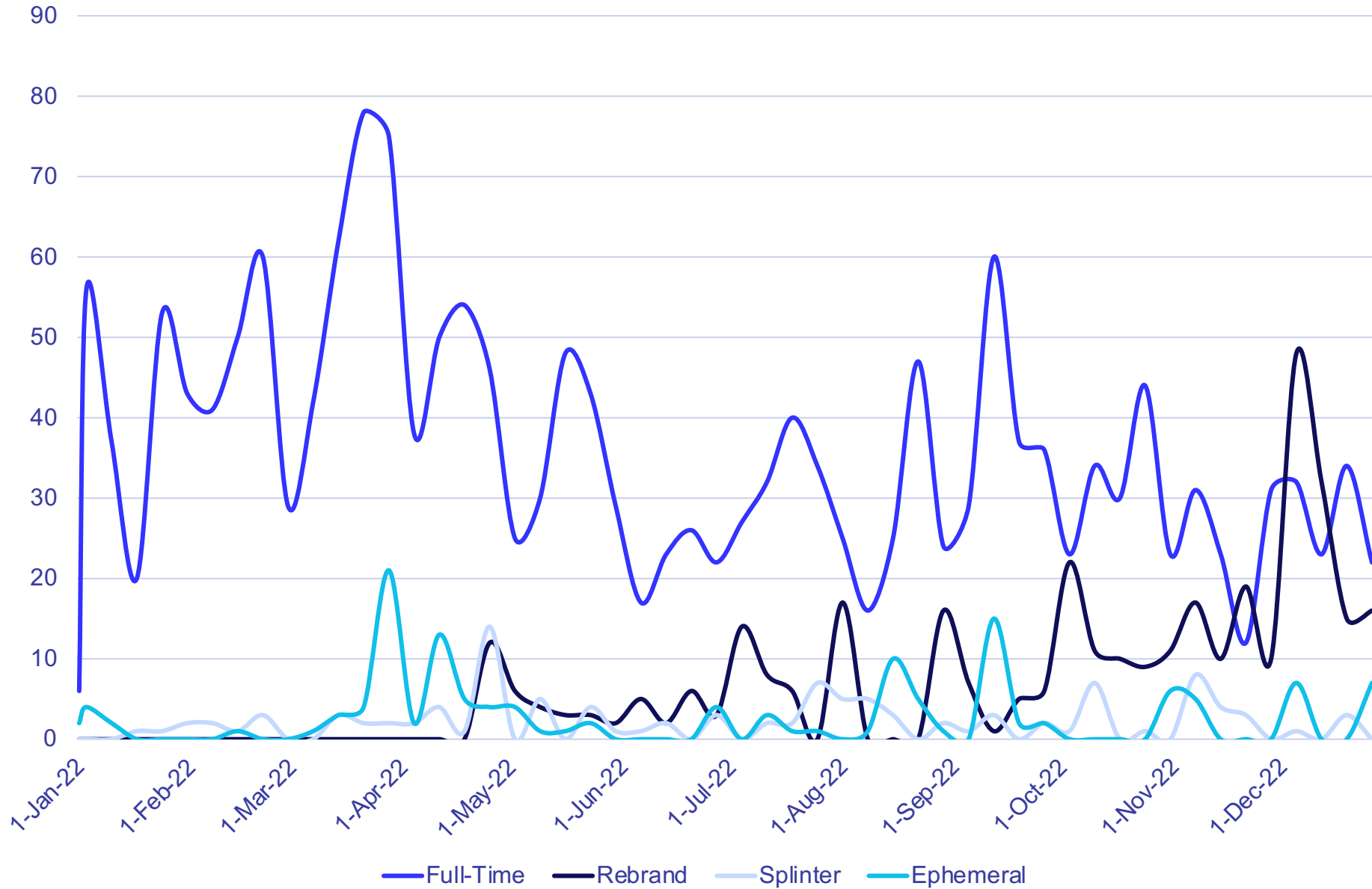
Sparta Blog

BLACK SUIT

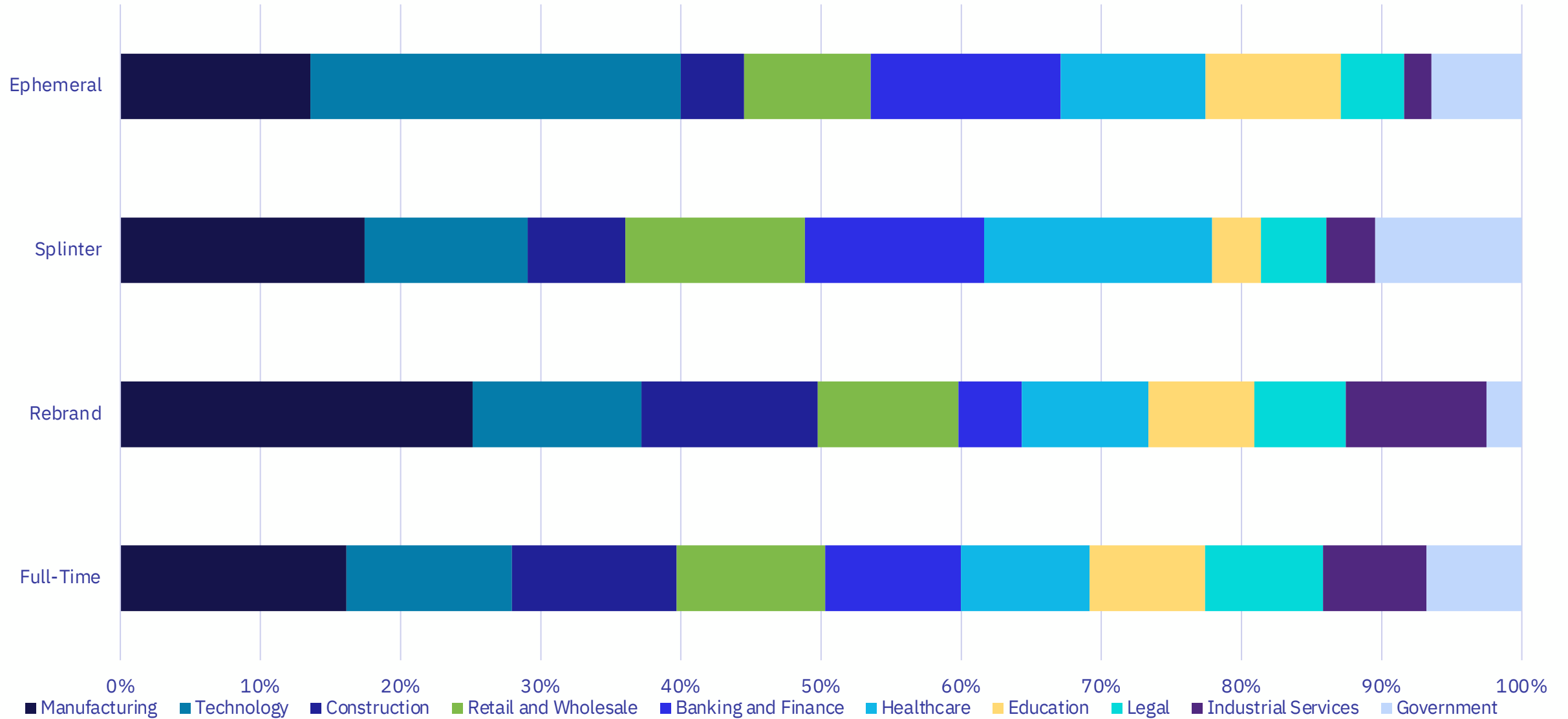
Ephemeral

Rebrand

Rate of Publicly Posted Ransomware Victims by Group Type (2022)



Industry Targeting by Group Type



BUT WHY

REBRAND RANSOMWARE?

The Five D's of Rebranding

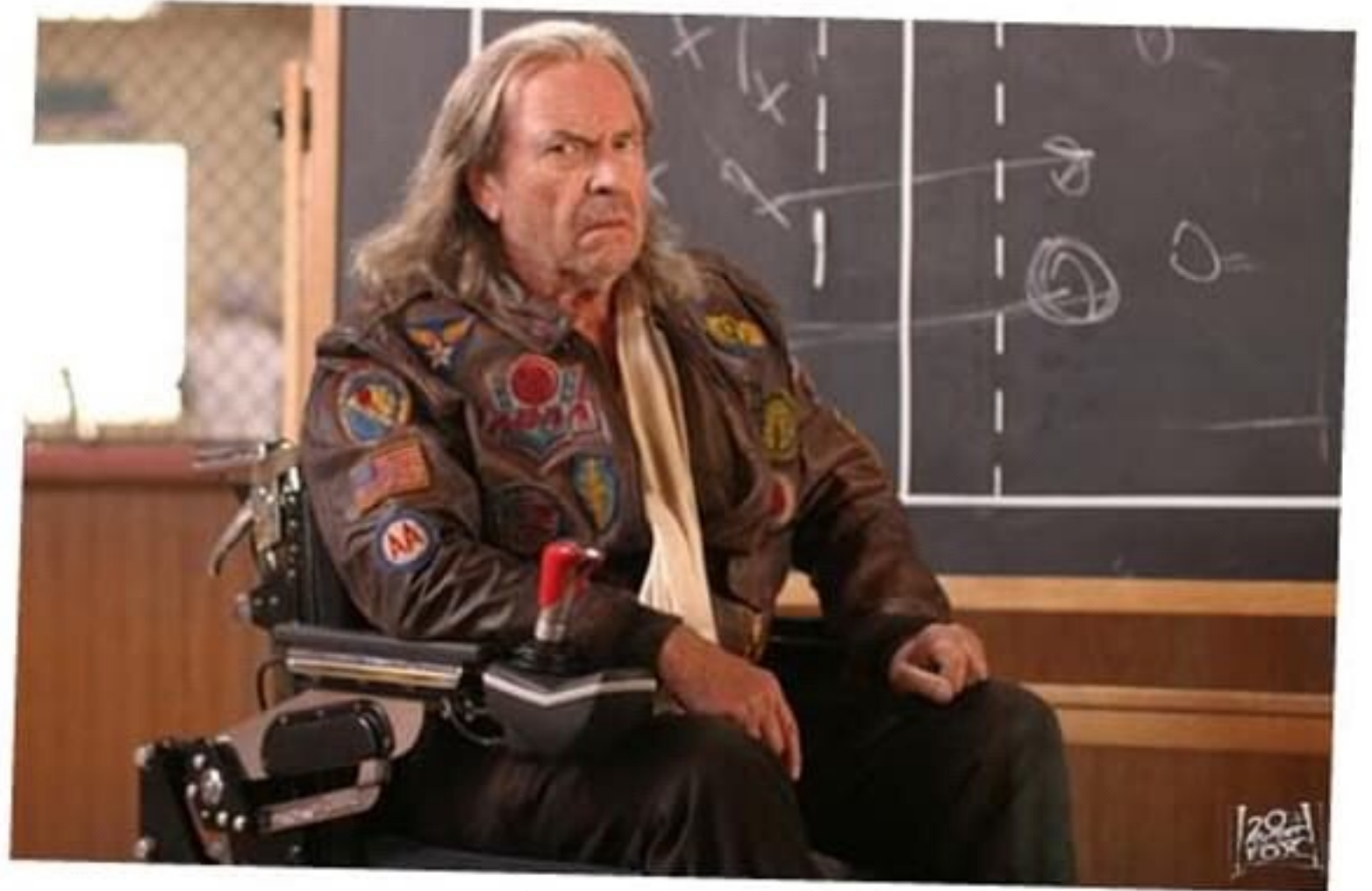
Dodge

Duck

Dip

Dive

Dodge



Patches O'Houlihan: Seven Time ADA All-Star

Rebranding's Effects on the Blue Team

- ✓ Another group to track and categorize
- ✓ Another leak site to scrape
- ✓ More behaviors and TTPs to learn
- ✓ A never-ending cycle of intelligence gathering

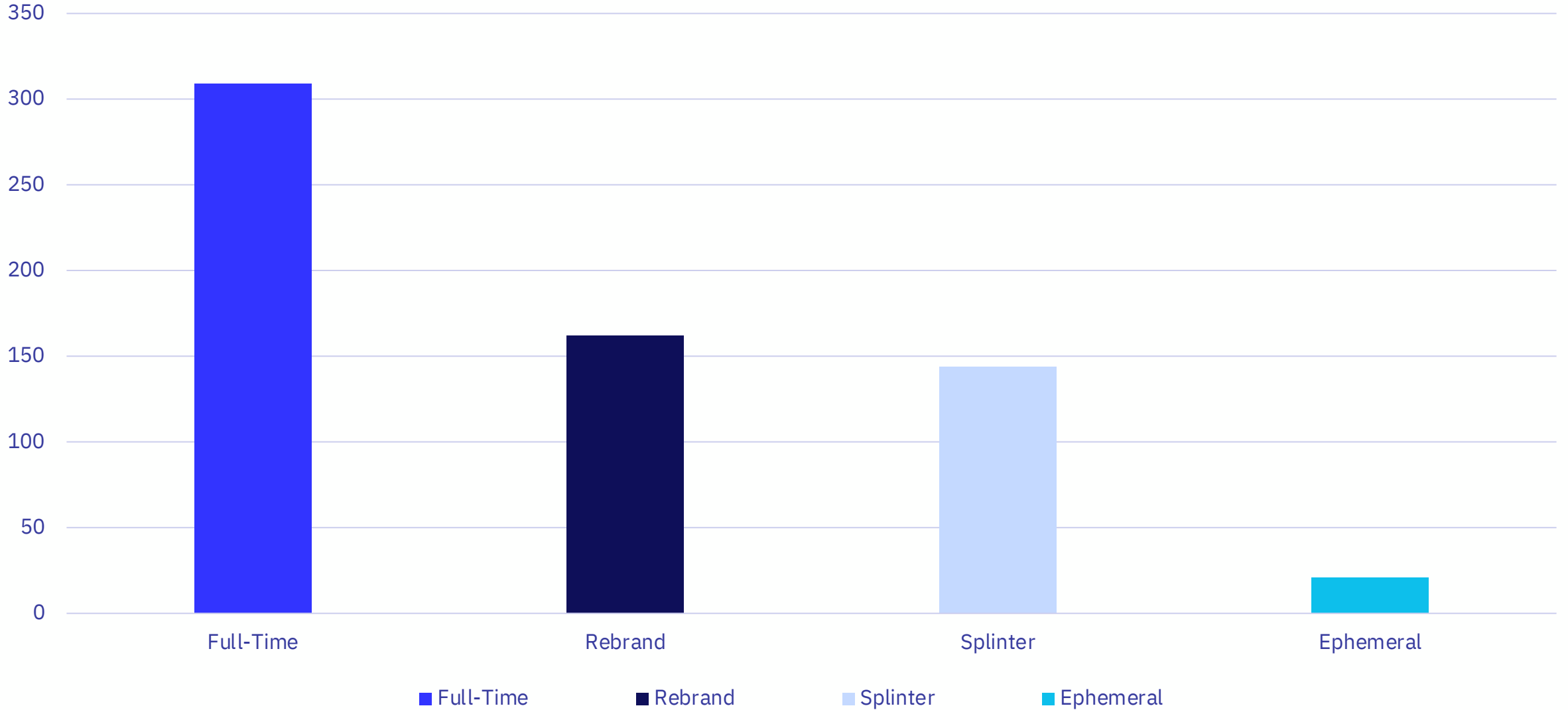


CASE STUDIES



IN RANSOMWARE REBRANDING

Average Operating Duration by Group Type (2022)



Case Study: DarkSide to BlackMatter to AlphV



Colonial Pipeline Attack
May 6, 2021

BlackMatter Shutdown Message (“Pressure from Authorities”)
November 2, 2021

- Rebrand Statistics:**
- First Rebrand Dwell Time: < 60 days
 - Second Rebrand Dwell Time: < 30 days

Extended Operations by 400+ days

Case Study: EvilCorp



Rebrand Observations:

- Rebrands often overlapped with each other
- Rebrand cadence became more frequent

Average Rebrand Duration: 38 days

Extended Operations by 400+ days

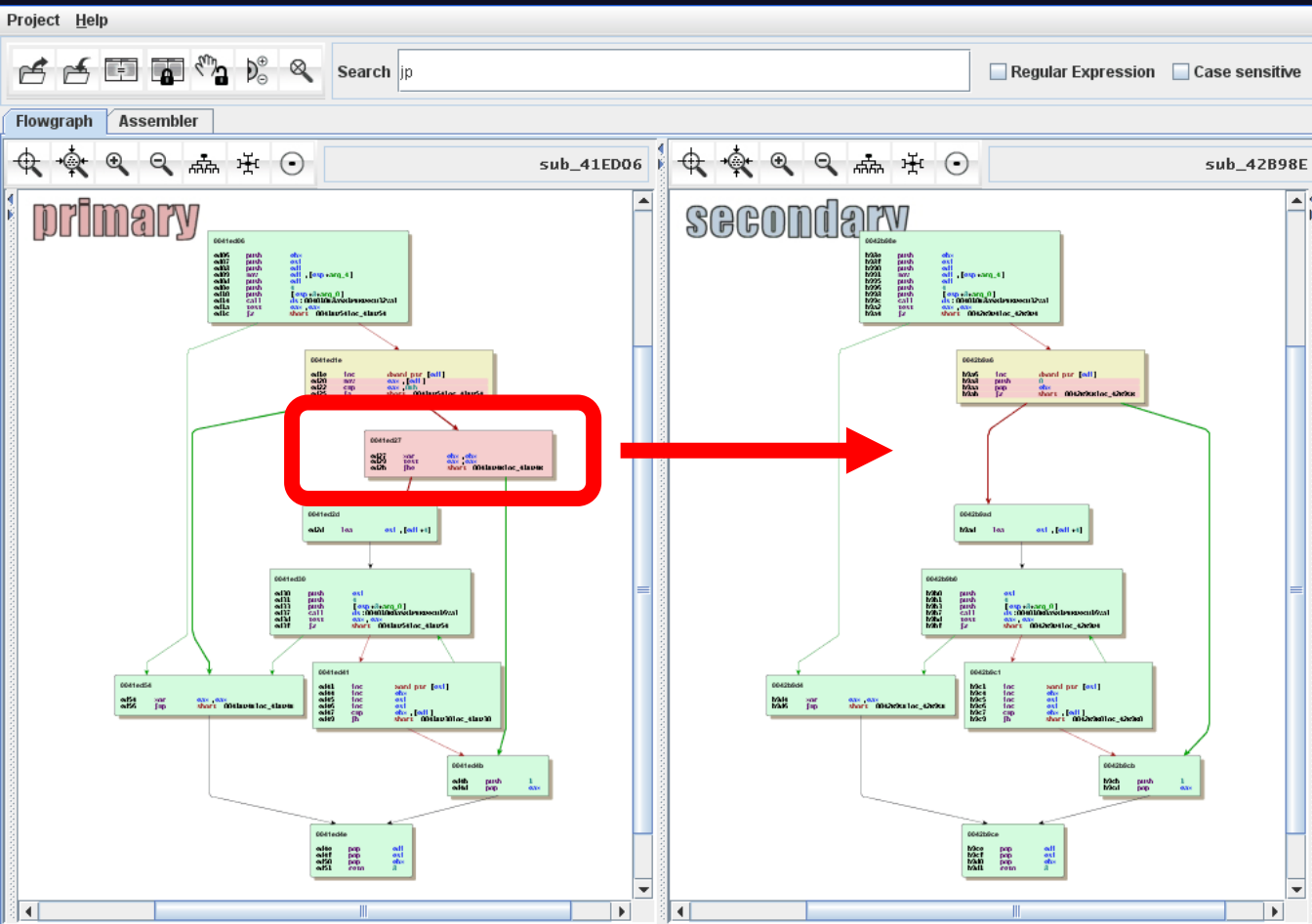


How to Spot a Rebrand

- File and Drive Enumeration
- Encryption Routines
- API Hashing/Importing Routines
- Proxy and Network Communication
- Control Flow
- Packing Routines



**SANCTIONS BE DAMNED |
FROM DRIDEX TO MACAW,
THE EVOLUTION OF EVIL CORP**



```

int WINAPI WinMain(
    HINSTANCE hInstance,
    HINSTANCE hPrevInstance,
    LPSTR lpCmdLine,
    int nShowCmd
)
{
    api::InitializeApiModule();
    api::DisableHooks();

    HANDLE hLocalSearch = NULL;
    filesystem::DRIVE_LIST DriveList;
    network_scanner::SHARE_LIST ShareList;

    TAILQ_INIT(&g_WhitelistPids);
    TAILQ_INIT(&DriveList);
    TAILQ_INIT(&ShareList);
    TAILQ_INIT(&g_PathList);
    TAILQ_INIT(&g_HostList);


    HANDLE hMutex = pCreateMutexA(NULL, TRUE, OBFA("kjsidugidf99439"));
    if ((DWORD)pWaitForSingleObject(hMutex, 0) != WAIT_OBJECT_0) {
        return EXIT_FAILURE;
    }
}

```

Conti Source Code Leak

Look for Code Reuse!

Don't Forget About Leak Sites



LEAKED DATA

<div style="background-color: #e0ffe0; padding: 5px; border: 1px solid green; margin-bottom: 10px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> [redacted].com </div> <div style="text-align: center; border: 1px solid green; padding: 2px; margin: 5px 0; font-weight: bold; color: green;">PUBLISHED</div> <p>Founded in 1942, [redacted] is a company that manufactures safety marking products and engineered films such as barricade tapes, marking flags, marking whisksers, and roll</p> <div style="display: flex; justify-content: space-between; align-items: center; font-size: 0.8em;"> Updated: 16 Jan, 2023, 18:47 UTC 12007 </div> </div>	<div style="background-color: #ffe0e0; padding: 5px; border: 1px solid red; margin-bottom: 10px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> [redacted].br </div> <div style="text-align: center; border: 1px solid red; padding: 2px; margin: 5px 0; font-weight: bold; color: white;">17D 02h 07m 14s</div> <p>Fundada em [redacted] em modestas instalações com a força de um jovem empreendedor que acreditou e viu a oportunidade de mudar sua vida e ao</p> <div style="display: flex; justify-content: space-between; align-items: center; font-size: 0.8em;"> Updated: 16 Jan, 2023, 11:53 UTC 317 </div> </div>
<div style="background-color: #ffe0e0; padding: 5px; border: 1px solid red; margin-bottom: 10px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> [redacted].com.tr </div> <div style="text-align: center; border: 1px solid red; padding: 2px; margin: 5px 0; font-weight: bold; color: white;">18D 01h 38m 38s</div> <p>ULUGÜN, General Manager Mr. Cemil ÇAĞLARKAYA, Balcan ÇAĞLARKAYA, Bora ULUGÜN Agency Manaqer title. We are</p> <div style="display: flex; justify-content: space-between; align-items: center; font-size: 0.8em;"> Updated: 16 Jan, 2023, 11:25 UTC 314 </div> </div>	<div style="background-color: #ffe0e0; padding: 5px; border: 1px solid red; margin-bottom: 10px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> [redacted].com.sa </div> <div style="text-align: center; border: 1px solid red; padding: 2px; margin: 5px 0; font-weight: bold; color: white;">16D 04h 55m 48s</div> <p>[redacted] is one of the leading retail companies in the Middle East offering the reputed brands from across the world with finest product & customer service.</p> <div style="display: flex; justify-content: space-between; align-items: center; font-size: 0.8em;"> Updated: 16 Jan, 2023, 10:42 UTC 314 </div> </div>

```

<div class="countup-block">
  <div class="countup-title">We've been working since September 3, 2019</div>
  <div class="countup" id="countup1">
    <span class="timeel years">00</span>
    <span class="timeel timeRefYears">years</span>
    <span class="timeel days">00</span>
    <span class="timeel timeRefDays">days</span>
    <span class="timeel hours">00</span>
    <span class="timeel timeRefHours">hours</span>
    <span class="timeel minutes-countup">00</span>
    <span class="timeel timeRefMinutes">minutes</span>
    <span class="timeel seconds-countup">00</span>
    <span class="timeel timeRefSeconds">seconds</span>
  </div>

  <div class="row">
    <div class="col-md-12">
      <a href="/bug-bounty" class="bugbounty-link">Web Security & Bug Bounty</a>
    </div>
  </div>

<script src="/public/js/sweetalert2.all.min.js"></script>
<script src="/public/timer/countup/jquery.countup.js"></script>
<script src="/public/timer/js/script.js"></script>
<script src="/public/js/bootstrap.bundle.min.js"></script>
<script src="/public/js/modal.js" type="text/javascript"></script>

```

Websites are Code too!

Signatures, Detections, Definitions... Oh My!



Profiling Behaviors

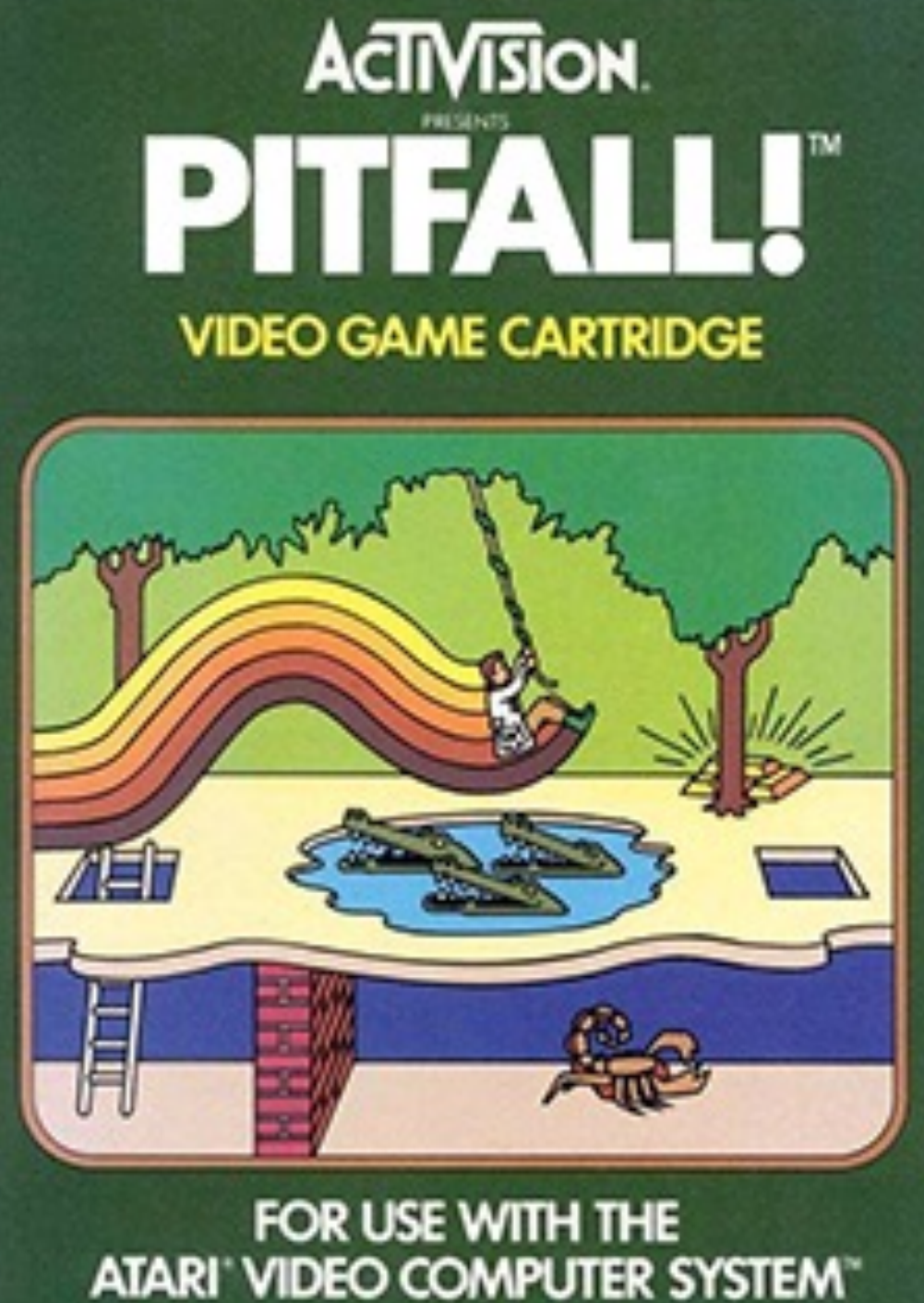
- Tactics, Techniques, Procedures
 - Initial Intrusion
 - Post-Exploitation
- Negotiation Tactics
- Dark Web Identities
- Communication Style and Phrase Reuse
- Rebrand Intervals
- Financial Behaviors
- Relationships with Other eCrime Groups

Develop a “Living” Threat Profile!



Watch Out! The Ransomware Ecosystem is Vast!

- Quick attribution to a known group
 - The actual core group vs the extended group often referenced by media
 - RaaS complicates things... A LOT
- Outsourcing happens
 - Code Reuse between Lockbit3 and BlackMatter
- Ransomware groups have leaks too
 - Conti Playbooks
 - Source Code
- Large groups have options, which makes our job harder... A lot harder



Case Study: BrightNight / Bl00dy

Observations:

- No traditional leak sites used in either case
 - Data leaked via Telegram or similar
- Overlapping email address used for negotiations
- Initial intrusion via exploitation of Paper Cut vulnerability
- Bl00dy leveraged leaked Lockbit 3.0 builder



What's the Point of All This?



Happy Hacker



Sad Hacker



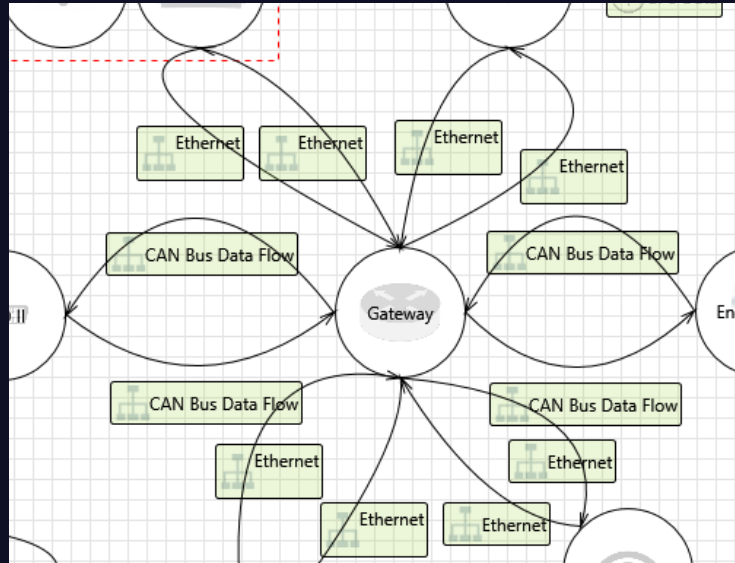
Communicate the Single Source of Truth



Key Characteristics of Effective Threat Intel Communication

- Consumable
- Actionable
- Highly Contextualized
- Relevant
- Timely
- Rate Limited
- Easily Understood

Model the Intelligence, Inform the Hunt



Threat Intel Sharing for the Win!

- Share Threat Profiles
- Share Tools and Techniques
- Share Emerging Trends and Research
- Share Datasets
- Share Analysis Notes
- Share it All

mobile

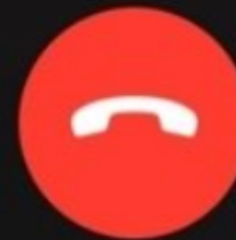
ACTION



Remind Me



Message



Decline



Accept



QUESTIONS?

Thank You

Drew Schmitt

GRIT Lead Analyst

Drew.Schmitt@GuidePointSecurity.com

Twitter: @5ynax (me), @GRIT_Intel (GRIT)

GuidePointSecurity.com/GRIT

