HOW CARBON SPIDER EMBRACED RANSOMWARE

ERIC LOUI
JOSH REYNOLDS

VB LOCALHOST 2021

CROWDSTRIKE

ERIC LOUI

Senior Intelligence Analyst

- Focused on eCrime campaign tracking
- Previously worked at Deloitte, U.S. Department of State
- Presented at SANS Cyber Threat Intelligence Summit, Fal.Con, ACoD

CROWDSTRIKE

JOSHUA REYNOLDS

Senior Security Researcher

- Focused on malware reverse engineering and intelligence analysis
- Presented at multiple BSides events, DEF CON and RSAC focusing on ransomware, malicious document analysis and cryptojacking malware
- Multiple community efforts, including co-authoring a malware analysis course for a local polytechnic school

AGENDA

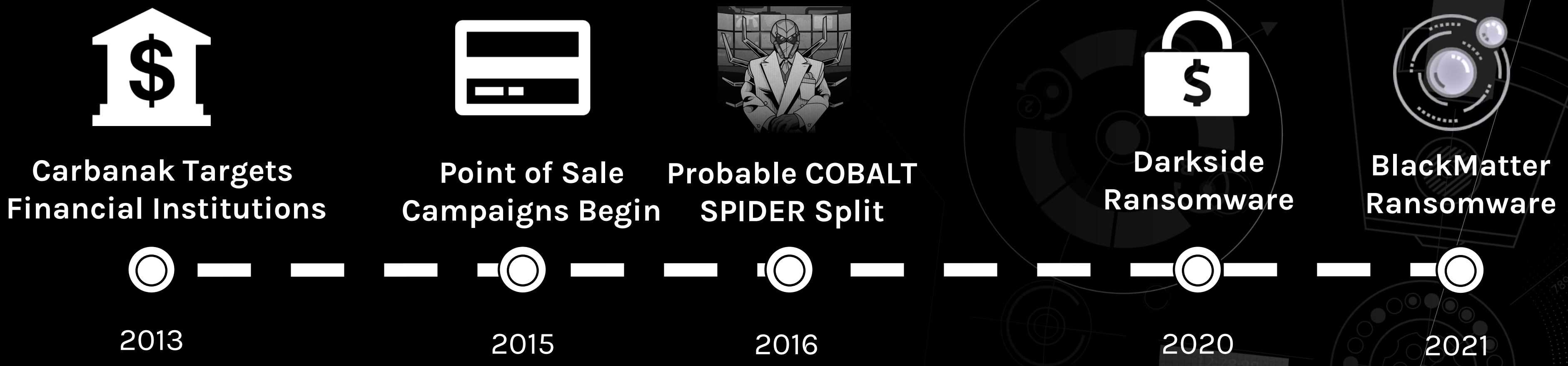
- Background
- Opportunistic Malware Delivery
- New Tooling
- Post-Access TTPs
- Darkside
- BlackMatter

CARBON SPIDER

ORIGIN AND BACKGROUND

WHO IS CARBON SPIDER?

FROM CARBANAK TO DARKSIDE AND BLACKMATTER



Carbanak Targets Financial Institutions

2013

Point of Sale Campaigns Begin

2015

Probable COBALT SPIDER Split

2016

Darkside Ransomware

2020

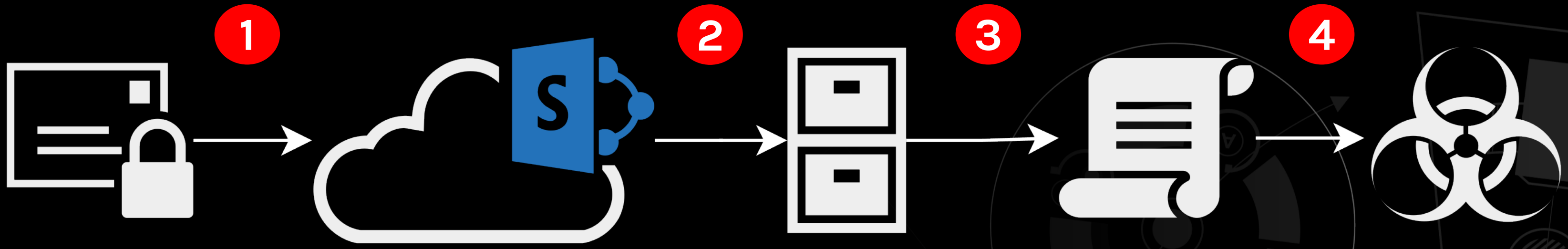
BlackMatter Ransomware

2021

Historical CARBON SPIDER Malware				
Carbanak aka Sekur	Agent ORM	JS Flash	Bateleur	GRIFFON aka Harpy

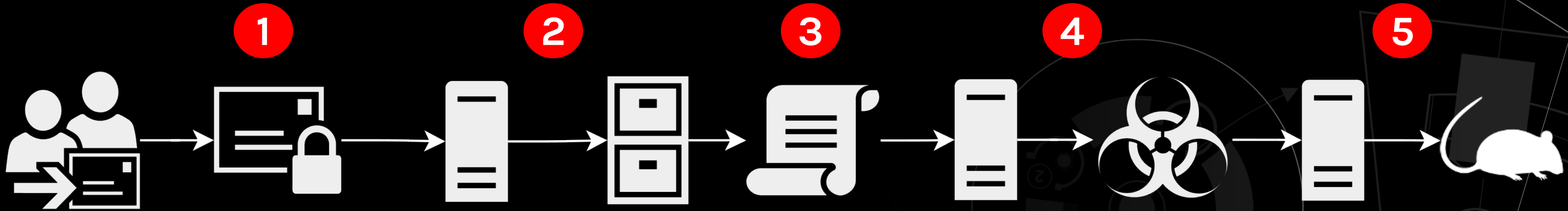
APRIL 2020: OPERATIONAL SHIFT

OPPORTUNISTIC DOMENUS CAMPAIGNS DELIVER HARPY



1. Large-scale phishing campaigns contain links to compromised SharePoint sites
2. Users download ZIP archives
3. Archives contain Domenus VBS; later Domenus JS, Domenus Stager
4. Domenus downloads Harpy backdoor

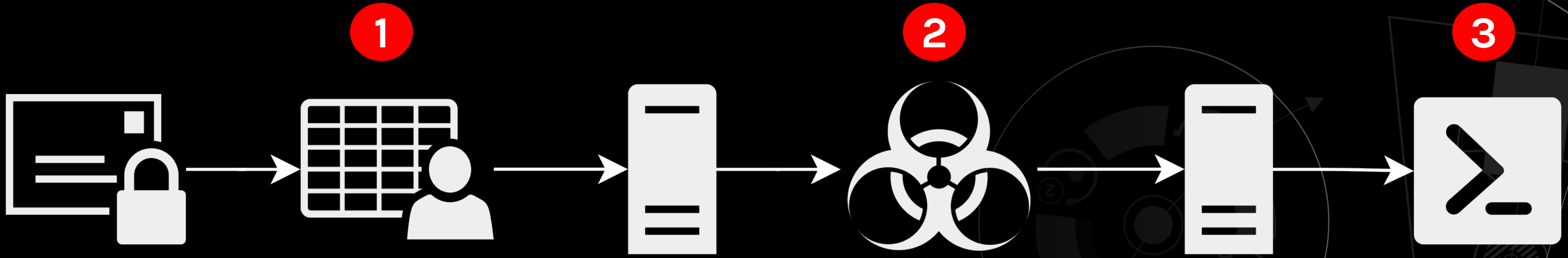
INTRODUCTION OF JSS LOADER TO DELIVER SEKUR



1. Probable compromise of email distribution service enables mass spam campaign
2. Links lead to remote ZIP archive
3. Archive contains Leo VBS
4. Leo VBS downloads JSS Loader
5. JSS Loader downloads Custom Sekur PowerShell stager

CROWDSTRIKE

RELATIONSHIP WITH ZLOADER OPERATOR ENABLES KILLACK DISTRIBUTION



1. Generic spam campaigns deliver Excel workbooks
2. Workbooks contain macro code to download Zloader
3. Zloader downloads KillACK PS backdoor from C2

CROWDSTRIKE

NEW TOOLING

ORIGIN AND BACKGROUND

JSS LOADER

- .NET version first observed in August 2019
- C++ version first observed in May 2021
- Supports delivery of PE, DLLs, VBS, JS and PowerShell

DOMENUS

- Observed in March 2020 using C2 domenuscdm[.]org to deliver Harpy
- VBS and JS stagers were introduced to deliver complex Domenus versions written in JS and VBS
- Collects system info, domain info, web history and screenshots
- Supports delivery of PowerShell, PE and DLL files
- Domenus PS was later delivered by Domenus VBS in April 2021

KILLACK

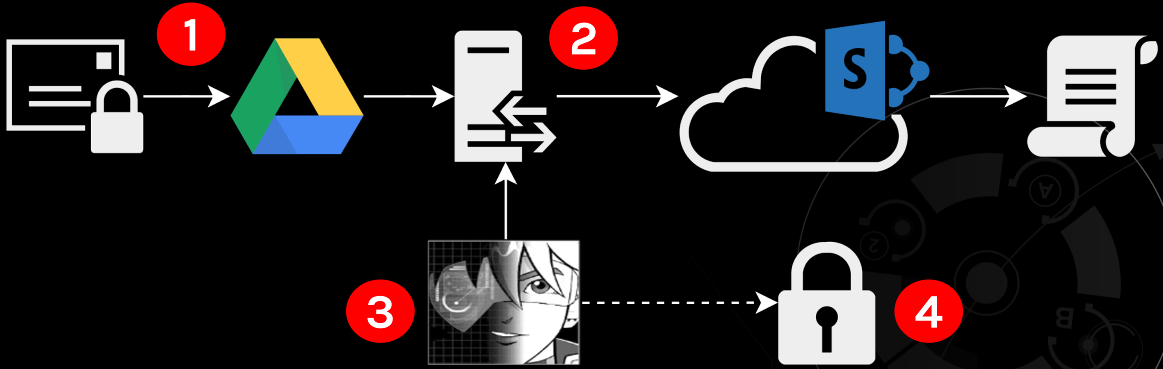
- PowerShell backdoor first observed in June 2020
- Executes PS through a job queue with output to C2
- Supports multiple modules used for bypassing AMSI, self-propagation, information gathering and execution of Cobalt Strike stagers

DEMUX

- Custom PowerShell loader used to reflectively load DLLs
- Observed loading Sekur stagers, Sekur, PILLOWMINT, and Cobalt Strike stagers

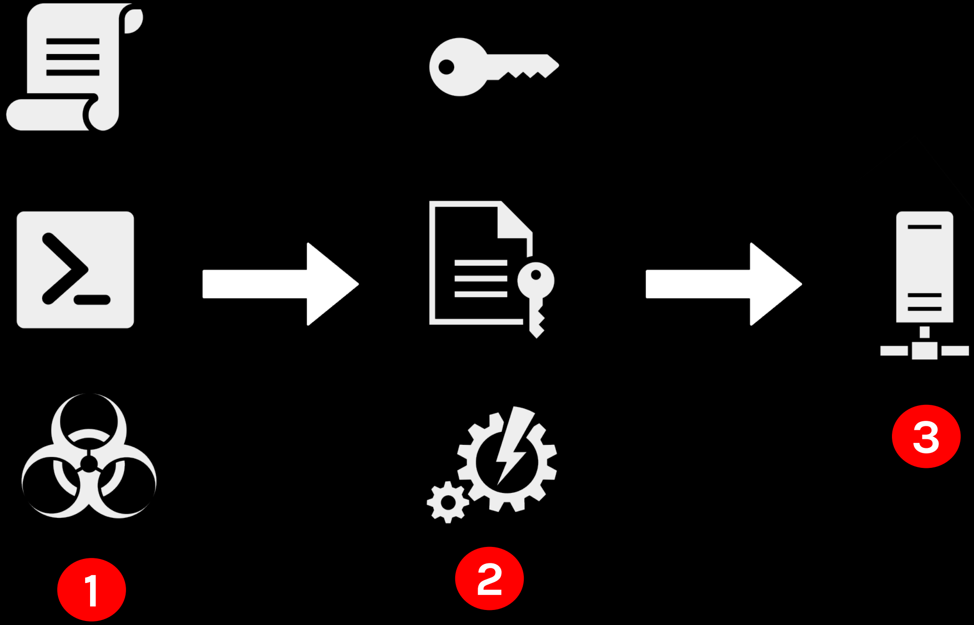
RANSOMWARE

REVIL CAMPAIGNS



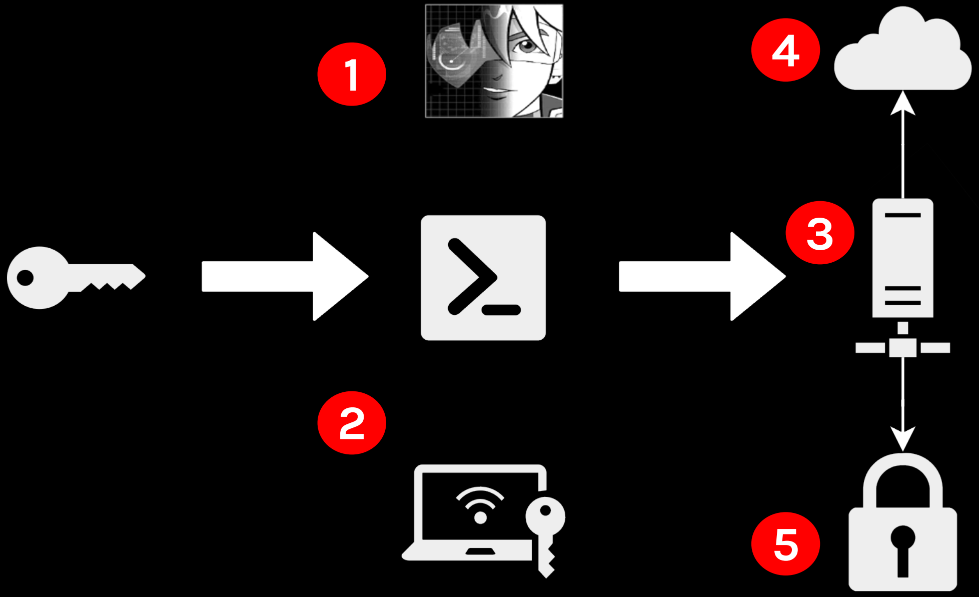
1. Phishing campaign uses Google Docs link
2. Link leads to redirect to SharePoint site hosting Domenus VBS
3. Server hosting redirect also used as Cobalt Strike C2
4. Related Cobalt Strike samples used in multiple REvil campaigns

DARKSIDE CAMPAIGNS



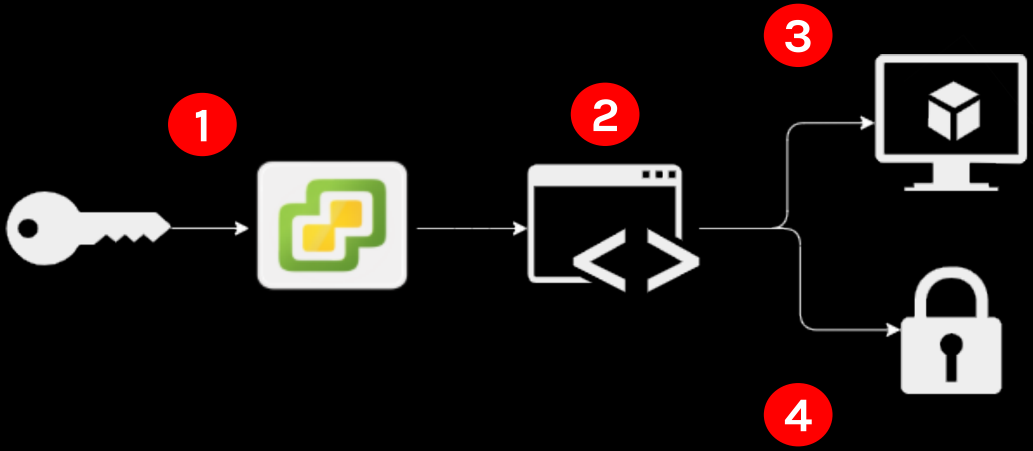
1. Initial foothold: Harpy, KillACK, or Sekur
2. Credential Access:
    1. Passwords from memory
    2. NTDS.DIT capture
    3. CVE-2020-1472 exploitation
3. Lateral movement using RDP or SSH

DARKSIDE CAMPAIGNS, CONTINUED



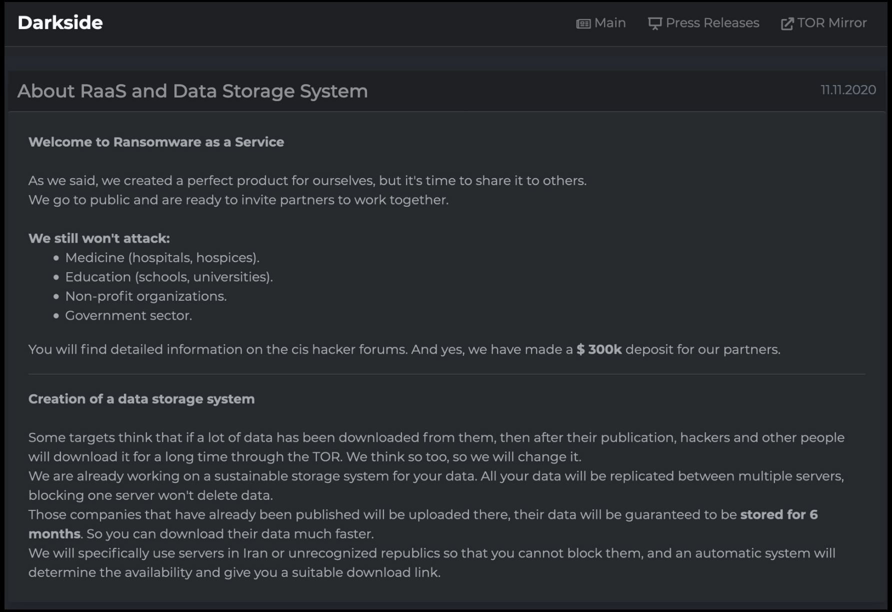
1. Using credentials, deploy Cobalt Strike throughout network
2. Occasionally augment Cobalt Strike with KillACK, Plink, GoToAssist
3. Harvest data, compress into archives
4. Exfiltrate to MEGA; victim files posted on Tor dedicated leak site
5. Deploy Darkside Ransomware

ESXI RANSOMWARE DEPLOYMENT



1. Using valid credentials, authenticate to vSphere
2. Enable SSH access, log in via SSH
3. Terminate running VMs
4. Execute Darkside ELF binary

RANSOMWARE-AS-A-SERVICE AFFILIATE PROGRAM



About RaaS and Data Storage System

11.11.2020

Welcome to Ransomware as a Service

As we said, we created a perfect product for ourselves, but it's time to share it to others.
We go to public and are ready to invite partners to work together.

We still won't attack:

- Medicine (hospitals, hospices).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

You will find detailed information on the cis hacker forums. And yes, we have made a **$ 300k** deposit for our partners.

Creation of a data storage system

Some targets think that if a lot of data has been downloaded from them, then after their publication, hackers and other people will download it for a long time through the TOR. We think so too, so we will change it.
We are already working on a sustainable storage system for your data. All your data will be replicated between multiple servers, blocking one server won't delete data.
Those companies that have already been published will be uploaded there, their data will be guaranteed to be **stored for 6 months**. So you can download their data much faster.
We will specifically use servers in Iran or unrecognized republics so that you cannot block them, and an automatic system will determine the availability and give you a suitable download link.

- 10 November 2020: Forum advertisements for RaaS affiliates; BTC deposited
- 11 November 2020: Announcement of RaaS program on Tor site
- Ransom notes direct victims to Tor portal
- 10-25% payout to CARBON SPIDER; commonly 20%

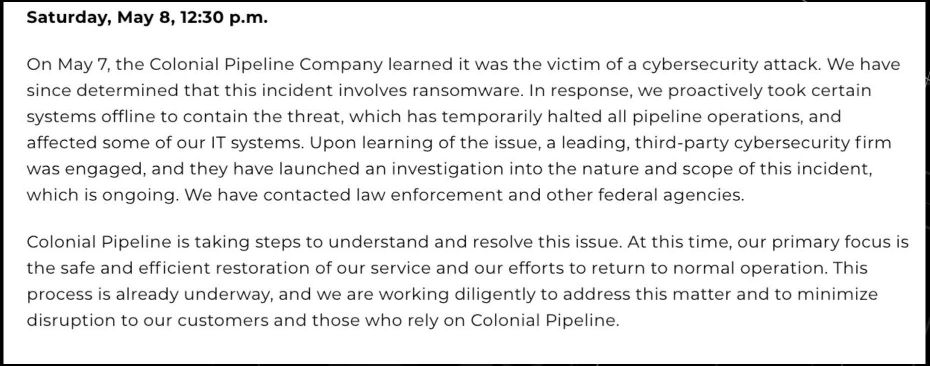
ATTRIBUTION TO CARBON SPIDER

- Numerous separate Darkside incidents attributed to CARBON SPIDER
  - DFIR artifacts indicate consistent TTPs
  - Use of unique / distinctive tooling
  - Infrastructure commonalities
- Low volume of Darkside campaigns prior to RaaS announcement
  - No atypical Darkside campaigns pre-announcement
- RaaS announcements indicate Darkside operated by single group

COLONIAL PIPELINE INCIDENT

INCIDENT TIMELINE

- 8 May 2021: Colonial Pipeline discloses ransomware attack; Darkside implicated
- 9 May 2021: ransom payment made
- Criminal ecosystem reacts:
  - XSS bans ransomware-related posts
  - PINCHY SPIDER (Revil), Avaddon vendor announce restrictions on specific sectors
- 14 May 2021: Darkside RaaS closed, infrastructure taken down
- 7 June 2021: DOJ announces BTC seizure of affiliate cut from Colonial Pipeline ransom payment



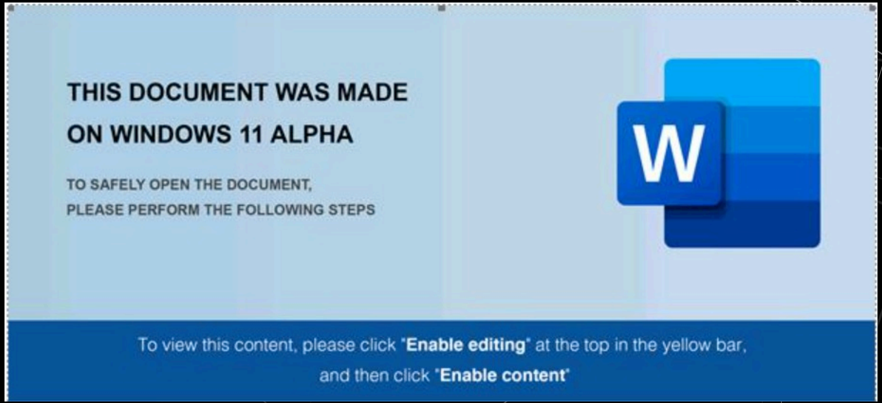
Saturday, May 8, 12:30 p.m.

On May 7, the Colonial Pipeline Company learned it was the victim of a cybersecurity attack. We have since determined that this incident involves ransomware. In response, we proactively took certain systems offline to contain the threat, which has temporarily halted all pipeline operations, and affected some of our IT systems. Upon learning of the issue, a leading, third-party cybersecurity firm was engaged, and they have launched an investigation into the nature and scope of this incident, which is ongoing. We have contacted law enforcement and other federal agencies.

Colonial Pipeline is taking steps to understand and resolve this issue. At this time, our primary focus is the safe and efficient restoration of our service and our efforts to return to normal operation. This process is already underway, and we are working diligently to address this matter and to minimize disruption to our customers and those who rely on Colonial Pipeline.

SUBSEQUENT CARBON SPIDER OPERATIONS

- 25 May 2021: SQL injection incident
- June 2021: JSS Loader, Harpy delivered via macro document phishing campaigns
- June 2021: probable CARBON SPIDER use of Hidden Tear ransomware following Sekur RAT and Demux DLL deployment
- July 2021: KillACK used alongside Cobalt Strike, NSM
- July 2021: BlackMatter unveiled



THIS DOCUMENT WAS MADE ON WINDOWS 11 ALPHA

TO SAFELY OPEN THE DOCUMENT, PLEASE PERFORM THE FOLLOWING STEPS

To view this content, please click "**Enable editing**" at the top in the yellow bar, and then click "**Enable content**"

BLACKMATTER

RECRUITING

- Forum post on 21 July 2021 to purchase access to corporate networks
- Targets in U.S., Canada, Australia, and the UK with >$100M USD in revenue
- 500-15,000 hosts
- No previous access

BLACKMATTER DARKSIDE OVERLAPS

BLACKMATTER WINDOWS DARKSIDE OVERLAPS

- Using aPLib to decompress configuration after decryption
- Overlaps in raw config format and config items, e.g:
  - Raw RSA-1024 public key
  - Key for C2 encryption
  - Config flags
  - Null-byte delimited Base64 config items
- Salsa20 to encrypt files with custom state matrix and protecting matrix with RSA-1024
- Using two HTTP C2 requests before and after encryption with system info and encryption stats
- Using WMI for shadow copy deletion

BLACKMATTER LINUX DARKSIDE OVERLAPS

- Red Hat Linux build environment
- Written in C++ and compiled using GCC with statically linked libcurl, Boost and CryptoPP libraries
- Overlaps in configuration items, e.g:
  - RSA-4096 public key
  - Extension allowlist
  - Thread count for encryption
  - Ransom note
  - Debug log file path
  - C2 domains to contact
- Performs C2 requests with cURL
- Stops ESXi machines and enumerates volumes

OUTLOOK

ECRIME SHIFT FROM CARDING OR BANKING TROJANS TO RANSOMWARE

- Numerous other eCrime actors have shifted operations to focus entirely on ransomware; CARBON SPIDER embodies this larger trend
- Similar to WIZARD SPIDER or INDRIK SPIDER all but abandoning banking fraud to conduct ransomware attacks
- Actors unlikely to shift back absent changes in economics
- eCrime actors capable of adapting to new trends and reinventing themselves

CROWDSTRIKE

THANK YOU!