



White Phoenix

Beating Intermittent Encryption




o Andy Thompson

Offensive Security Research Evangelist

- SSCP/CISSP
- GPEN
- Emcee of Dallas Hackers Association
- Travel Hacker

 andythompsoninfosec

 Andy_Thompson

 Andy.Thompson@CyberArk.com



CyberArk Labs Mission

Vulnerability Research

Malware/Breach Analysis

“Think like an attacker.”



CyberArk Labs

Publications

Open-Source Tools

Security Conferences



○ Agenda

- A brief history of ransomware.
- Intermittent Encryption
 - BlackCat Ransomware
- PDF 101 – Stream Objects
- White Phoenix + Demo





A Brief History of Ransomware



1989: PC Cyborg (aka The AIDS Virus)

- Replaced Autoexec.bat
 - After 90 days, Encrypted file names on c:/
- Asked to 'renew the license'
 - \$189 to a PO box in Panama
- Dr. Joseph Popp was arrested by Scotland Yard later that year and charged with blackmail



○ Ransomware Evolution

Lockers

- Early-2000's
- i.e. WinLock
 - Locks out of PC
- Easily removed
 - Boot into safe-mode
 - Remove registry key

Crypters

- Mid-2000's
- i.e. GPCoder
 - Encrypts individual files
- Not so easily removed
 - Required decryption key



○ Crypto-Currency (2009)

Bitcoin

- Secure
- Instant
- Not Regulated
- Pseudo-Anonymous
- Perfect for EXTORTION!



○ RaaS (2015)

- Allows individuals with little technical expertise to launch ransomware attacks
- Offers support and customer service
- Customized to target specific industries or organizations



◦ Double Extortion (2019)

- Encrypts AND exfiltrates data
- Double the pay! 💰💰
- Amplifies urgency
 - Reputational damage
 - Protection against backup recovery



○ Today's Ransomware



○ Intermittent Encryption

Speed

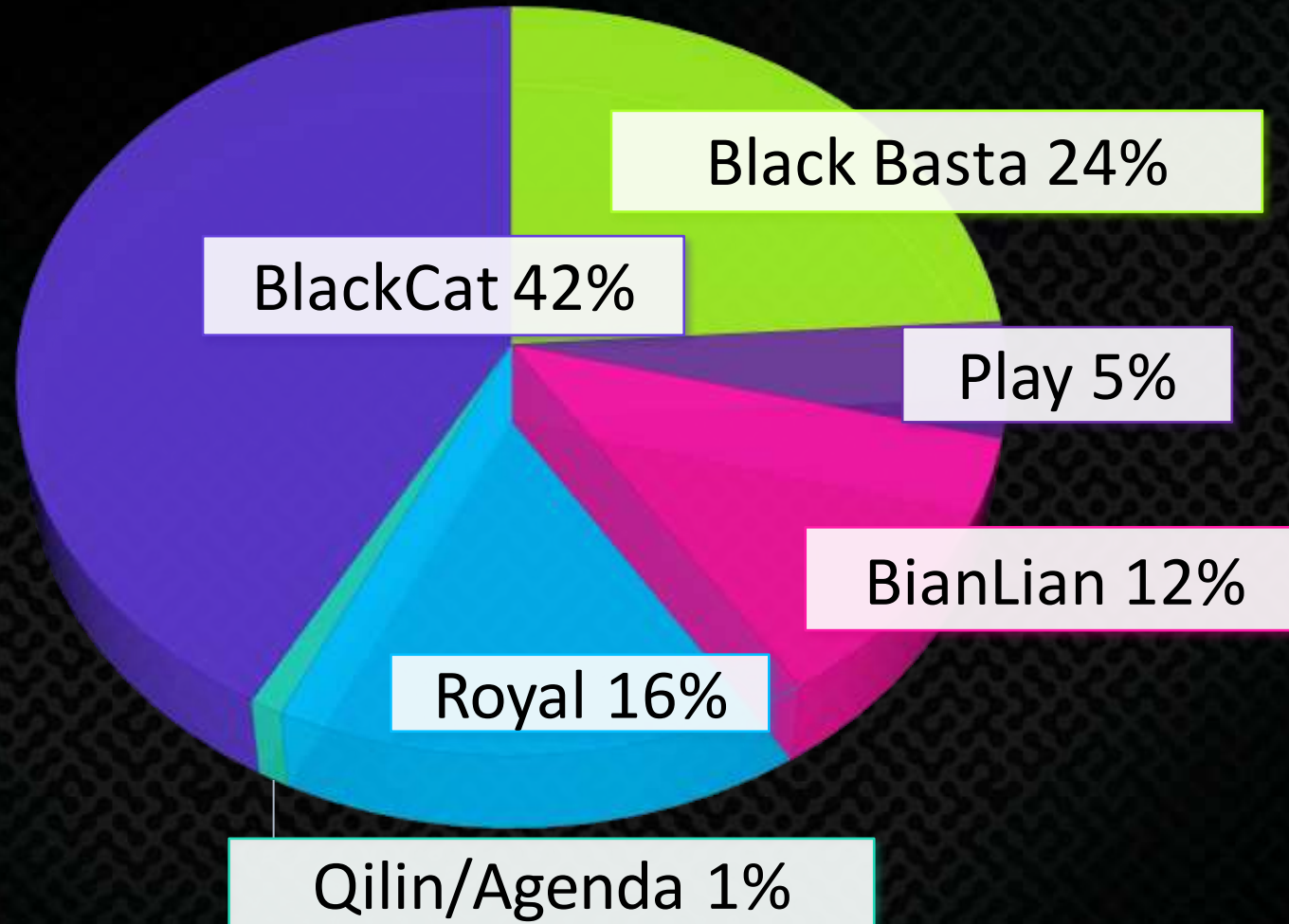
- Potentially Stopped Prematurely
- More Files = Higher Chance For Payment

Defense Evasion

- Avoid Detection
- Obfuscation



○ Telemetry



○ Blackcat

- Among the most successful RaaS
- “Most Sophisticated”
- Highly configurable
 - 6 Encryption modes



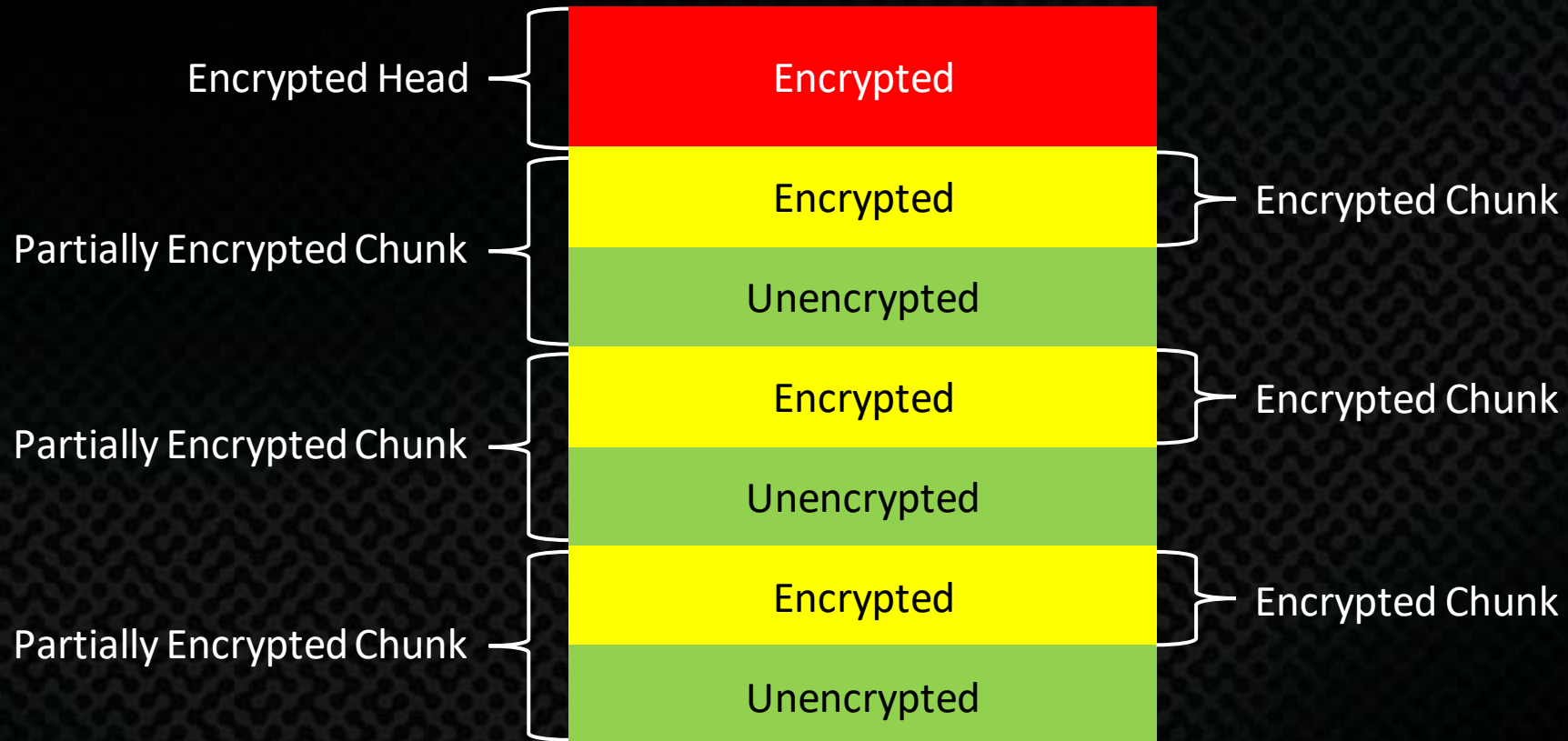
AUDIENCE

ADVISORY

TECHNICAL CONTENT



BlackCat Encryption Mode Structure



○ Encryption Modes 1 & 2



The diagram consists of two vertical rectangles. The left rectangle is solid red and contains the word 'Full' in white text. The right rectangle is divided into two horizontal sections: the top section is red and contains the text 'Head Only' in white, while the bottom section is light green and is empty.

Full

Head Only



○ Encryption Modes 3 & 4

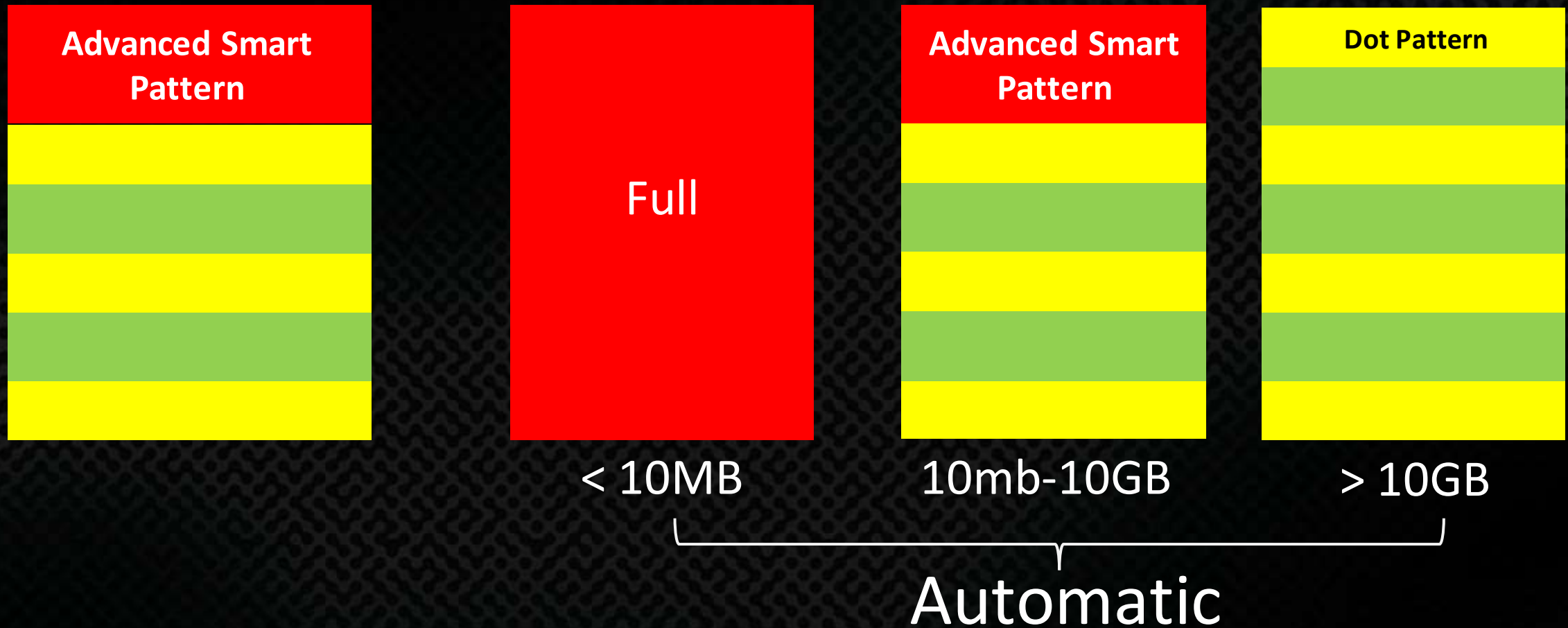
Dot Pattern



Smart Pattern



Encryption Modes 5 & 6



Anatomy of a PDF

Head
Body
Footer

```
4 0 obj
<</Filter/FlateDecode/Length 182>>
stream
xœmİOV T, @DLE ENO ðûÀ | ‡w- SO ëì º« , xđOR DC4
GS ¢C,, y² ¨¼? ´JA ‡æ8 <po ACK p SO i ê5 Å | ,, dEM ò² €W · SYN Ñ < é Á $ DLE %n- SYN ? ,, Õ ACK
ENO c Š DC1 EMEOT á ´ º Æ L p f < SI } ^ ò Ž = DC3 º | NUL ~ < ý ñ & f F $ q ý ò G É ; W J Ö Ð Z I € î
Ê ¤ g S # ô DC3 º ç ³ i " t ä t ñ à Â u > Ì / BS j | ã STX Ë DC3 º - S å Š ¼ § ¼ SOH " 11 p
endstream
endobj
```



○ This is an example

```
0 g
/GS8 gs
0 G
[(This is an)3( e)-3(xam)-5(p)3(le o)-7(f a )-2(sim)-3(p)3(le t)-3(ex)-3(t )] TJ
ET
Q
q
0.00000912 0 612 792 re
W* n
BT
/F1 11.04 Tf
1 0 0 1 228.17 709.66 Tm
0 g
0 G
[(o)-5(b)3(jec)-2(t)] TJ
ET
Q
q
0.00000912 0 612 792 re
W* n
BT
/F1 11.04 Tf
1 0 0 1 256.37 709.66 Tm
0 g
0 G
[( )] TJ
ET
Q
q
0.00000912 0 612 792 re
W* n
BT
/F1 11.04 Tf
1 0 0 1 258.89 709.66 Tm
0 g
0 G
[(in)5( a )-3(P)-4(D)-4(F)] TJ
ET
```

[(This is an)3(e)-3(xam)-5(p)3(le))]





White Phoenix



○ White Phoenix

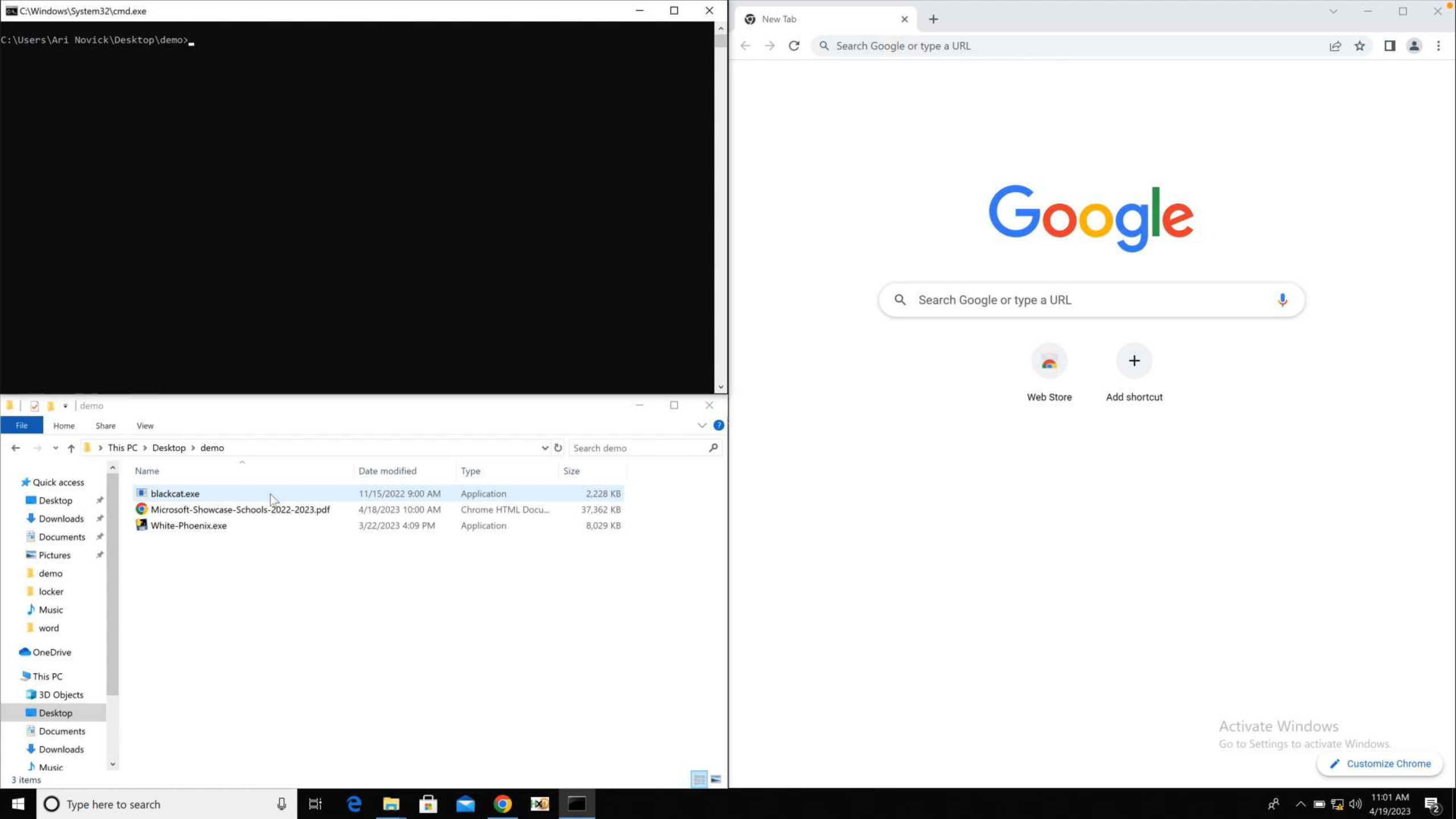
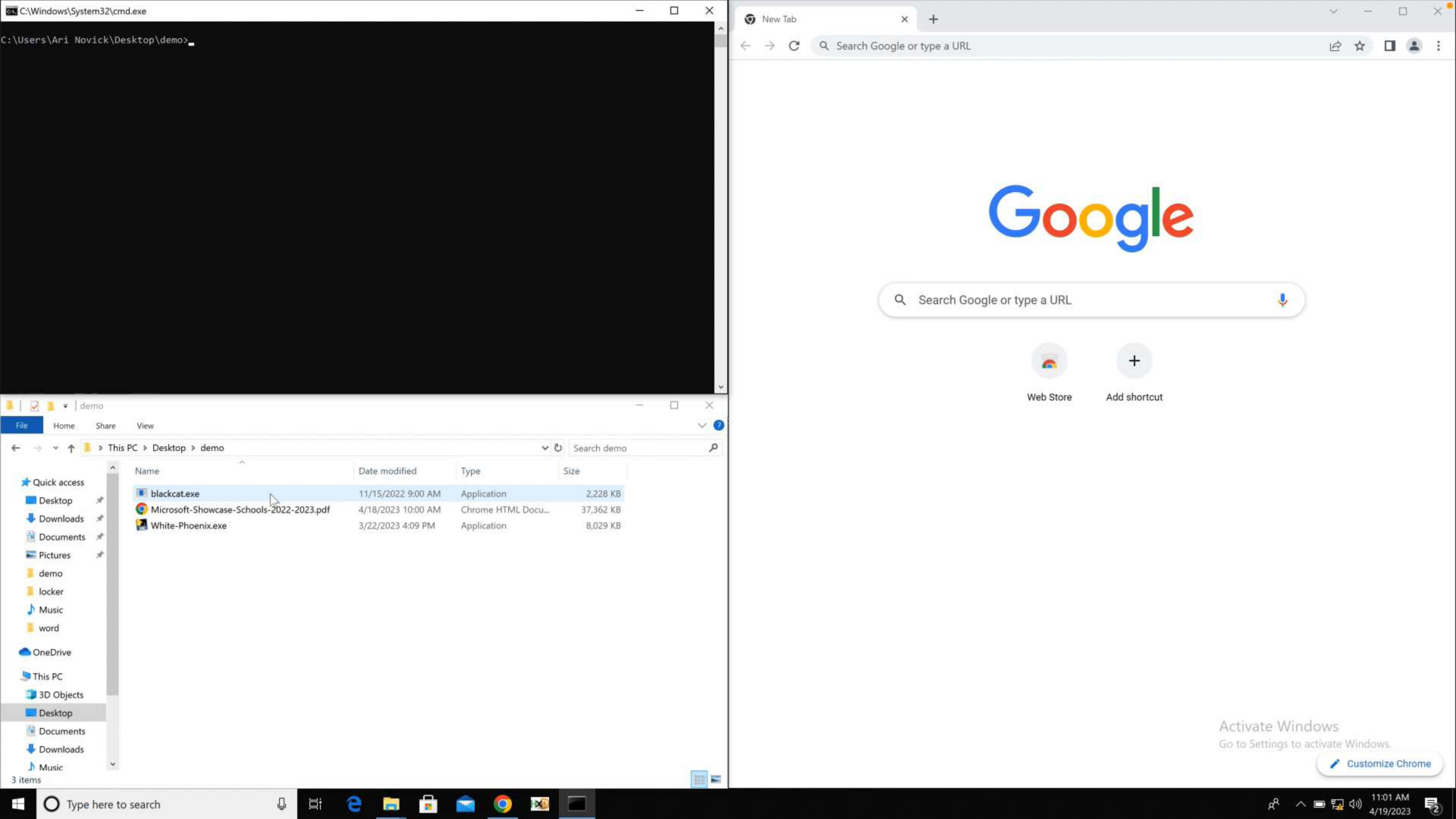
- Recovers data after intermittent encryption
- Primarily support PDFs
- Some support for office + zip



○ Recovery Logic

- Many Formats Composed Of Blocks
- Potentially Unencrypted Blocks
- Recover Content From Blocks With Data





Summary

- Intermittent Encryption = Partial Encryption
- Files Are Made Of Blocks
- We Can Recover Some Data





Blog Post



GitHub