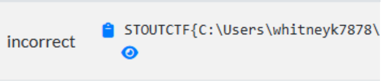
Tracking Down the Threat Actor's Malware Writeup

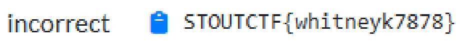
KAYNE

12/12/2025

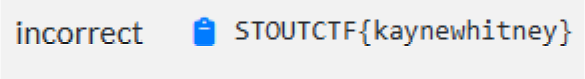
Hall of fame submissions:



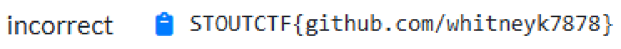
incorrect STOUTCTF{C:\Users\whitneyk7878\



incorrect STOUTCTF{whitneyk7878}



incorrect STOUTCTF{kaynewhitney}



incorrect STOUTCTF{github.com/whitneyk7878}

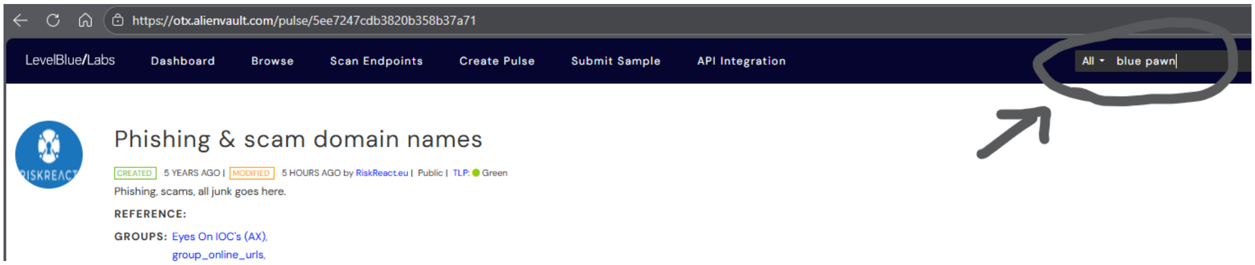
incorrect STOUTCTF{KayneWhitney}

I AM NOT THE THREAT ACTOR <3

Background: The spirit of this challenge was that we would continue hunting for this fictional threat actor called BluePawn. In the challenge before this, we discovered that blue pawn's malware had been posted to VirusTotal before. Continuing with the theme of using tools that Threat Intelligence experts use, (In order of challenges: Traditional OSINT, Virus Total, and now Alien Vault) we needed to start looking for more information on the threat actor.

1: Visit LevelBlue - Open Threat Exchange

2: Search for our threat actor:



https://otx.alienvault.com/pulse/5ee7247cdb3820b358b37a71

blue pawn

Phishing & scam domain names

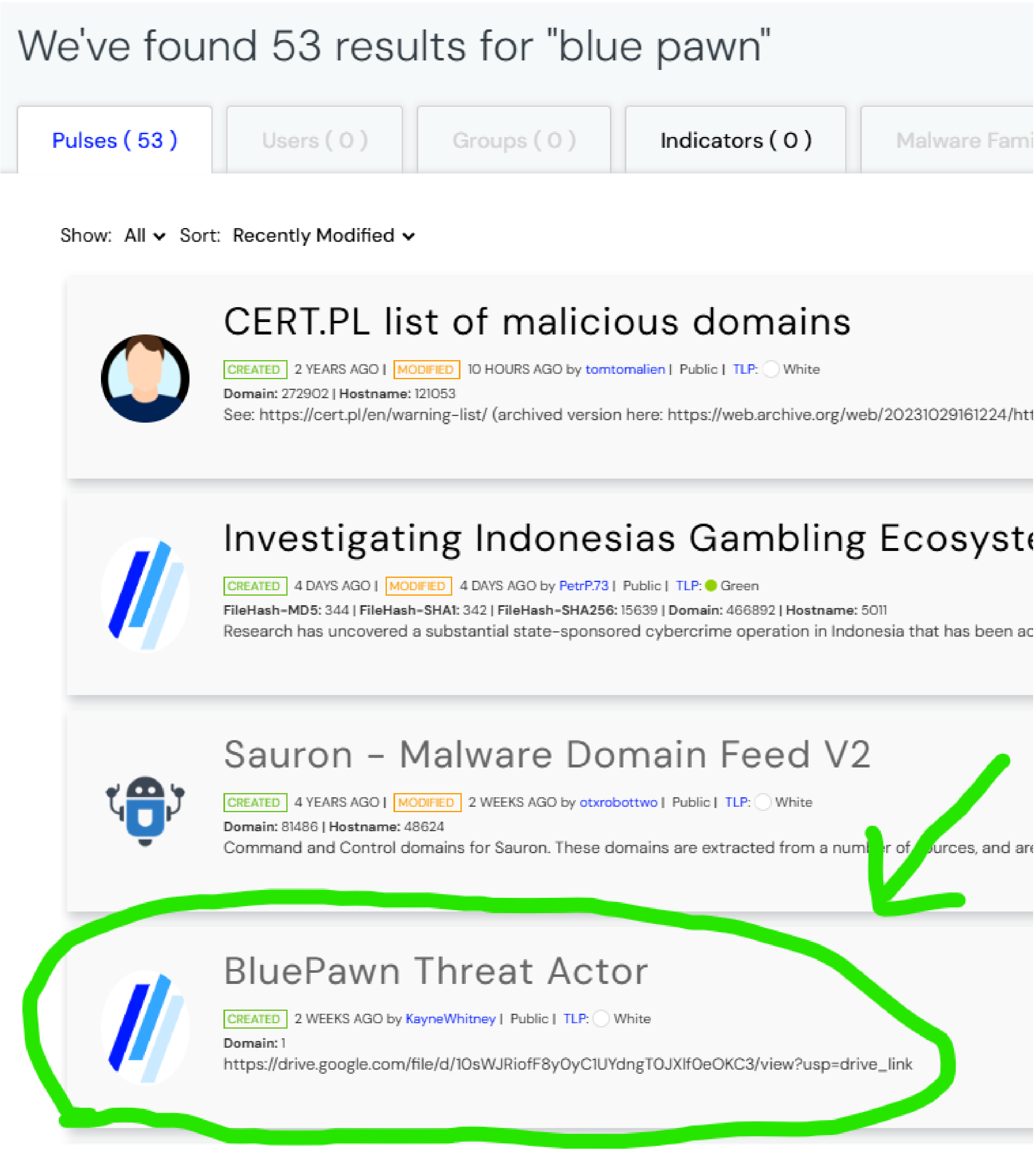
CREATED 5 YEARS AGO | MODIFIED 5 HOURS AGO by RiskReact.eu | Public | TLP: Green

Phishing, scams, all junk goes here.

REFERENCE:

GROUPS: Eyes On IOC's (AX), group_online_urls,

3: Whats this?



We've found 53 results for "blue pawn"

Show: All Sort: Recently Modified

CERT.PL list of malicious domains

CREATED 2 YEARS AGO | MODIFIED 10 HOURS AGO by tomtomalien | Public | TLP: ○ White

Domain: 272902 | **Hostname:** 121053

See: https://cert.pl/en/warning-list/ (archived version here: https://web.archive.org/web/20231029161224/htt

Investigating Indonesias Gambling Ecosyste

CREATED 4 DAYS AGO | MODIFIED 4 DAYS AGO by PetrP.73 | Public | TLP: ● Green

FileHash-MD5: 344 | **FileHash-SHA1:** 342 | **FileHash-SHA256:** 15639 | **Domain:** 466892 | **Hostname:** 5011

Research has uncovered a substantial state-sponsored cybercrime operation in Indonesia that has been ac

Sauron - Malware Domain Feed V2

CREATED 4 YEARS AGO | MODIFIED 2 WEEKS AGO by otxrobottwo | Public | TLP: ○ White

Domain: 81486 | **Hostname:** 48624

Command and Control domains for Sauron. These domains are extracted from a number of sources, and are

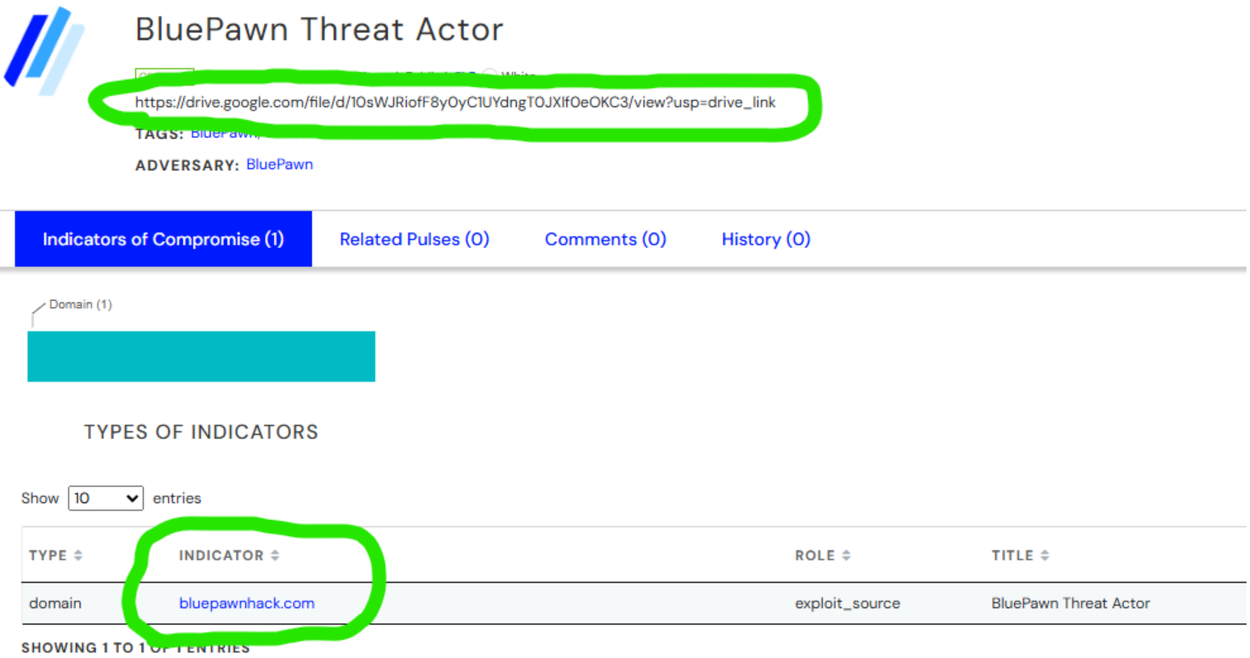
BluePawn Threat Actor

CREATED 2 WEEKS AGO by KayneWhitney | Public | TLP: ○ White

Domain: 1

https://drive.google.com/file/d/1OsWJRiofF8yOyC1UYdngTOJXlf0eOKC3/view?usp=drive_link

4: Now what do I investigate? The link or the indicator?



BluePawn Threat Actor

https://drive.google.com/file/d/10sWJRiofF8y0yC1UYdngT0JXlf0eOKC3/view?usp=drive_link

TAGS: BluePawn,

ADVERSARY: BluePawn

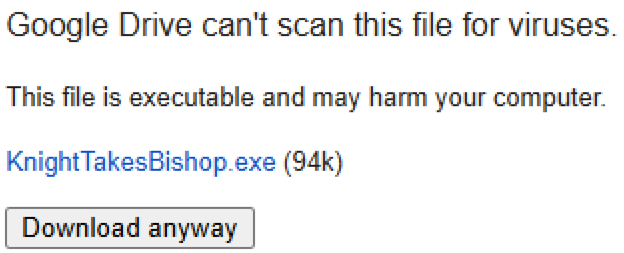
TYPES OF INDICATORS

Show 10 entries

TYPE	INDICATOR	ROLE	TITLE
domain	bluepawnhack.com	exploit_source	BluePawn Threat Actor

SHOWING 1 TO 1 OF 1 ENTRIES

5: Google Drive:



Google Drive can't scan this file for viruses.

This file is executable and may harm your computer.

KnightTakesBishop.exe (94k)

6: Reverse engineer this executable to find that there is a flag that gets put into memory during execution.