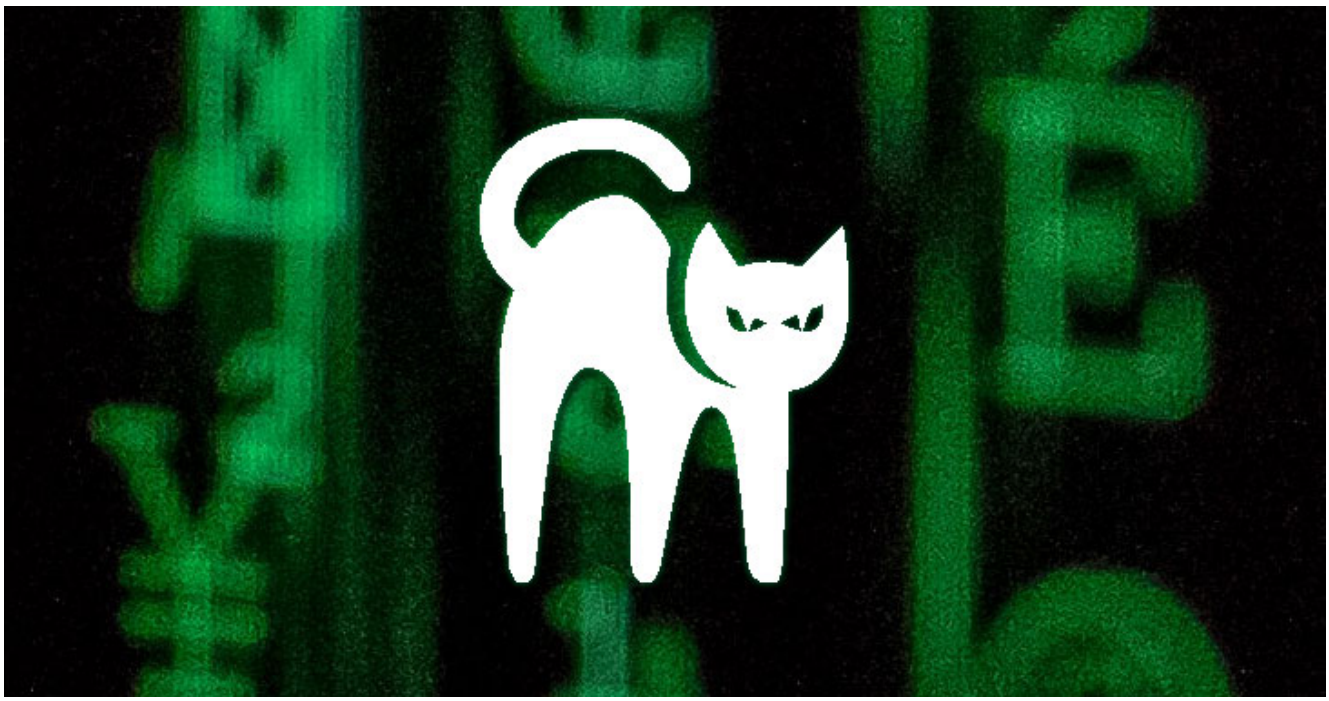
Researchers Connect BlackCat Ransomware with Past BlackMatter Malware Activity

thehackernews.com/2022/04/researchers-connect-blackcat-ransomware.html

April 8, 2022



Cybersecurity researchers have uncovered further links between BlackCat (aka ALPHV) and BlackMatter ransomware families, the former of which emerged as a replacement following international scrutiny last year.

"At least some members of the new BlackCat group have links to the BlackMatter group, because they modified and reused a custom exfiltration tool [...] and which has only been observed in BlackMatter activity," Kaspersky researchers said in a new analysis.

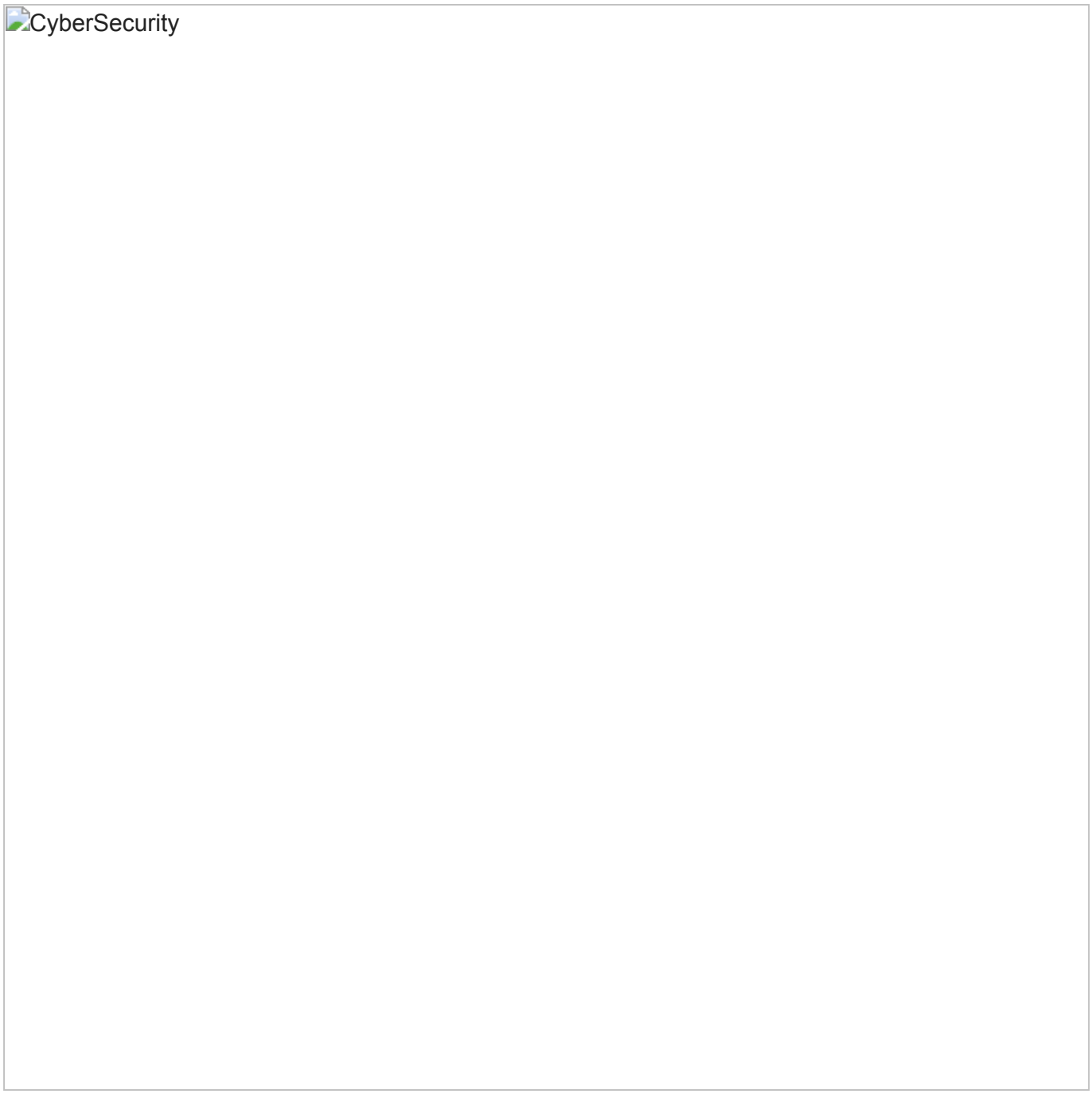
The tool, dubbed Fendr, has not only been upgraded to include more file types but also used by the gang extensively to steal data from corporate networks in December 2021 and January 2022 prior to encryption, in a popular tactic called double extortion.

The findings come less than a month after Cisco Talos researchers identified overlaps in the tactics, techniques, and procedures (TTPs) between BlackCat and BlackMatter, describing the new ransomware variant as a case of "vertical business expansion."

```
OPTIONS:
        --access-token <ACCESS_TOKEN>                Access Token
        --bypass <BYPASS>...
        --child                                      Run as child process
        --drag-and-drop                              Invoked with drag and drop
        --drop-drag-and-drop-target                  Drop drag and drop target batch file
    -h, --help                                       Print help information
        --log-file <LOG_FILE>                        Enable logging to specified file
        --no-net                                     Do not discover network shares on Windows
        --no-prop                                    Do not self propagate(worm) on Windows
        --no-prop-servers <NO_PROP_SERVERS>...       Do not propagate to defined servers
        --no-vm-kill                                 Do not stop VMs on ESXi
        --no-vm-kill-names <NO_VM_KILL_NAMES>...     Do not stop defined VMs on ESXi
        --no-vm-snapshot-kill                        Do not wipe VMs snapshots on ESXi
        --no-wall                                    Do not update desktop wallpaper on Windows
    -p, --paths <PATHS>...                           Only process files inside defined paths
        --propagated                                 Run as propagated process
        --ui                                         Show user interface
    -v, --verbose                                    Log to console
```

BlackCat stands out for two reasons: it's an affiliate actor that has deployed BlackMatter in the past and its malware is written in Rust, indicating how threat actors are increasingly pivoting to programming languages with cross-compilation capabilities.

The group "provides infrastructure, malware samples, ransom negotiations, and probably cash-out," the researchers noted. "Anyone who already has access to compromised environments can use BlackCat's samples to infect a target."



Once executed, the malware gets the Windows system's MachineGuid from the registry — a unique key generated during the installation of the operating system — as well as its UUID, before proceeding to bypass User Account Control (UAC), delete shadow backups, and start the encryption process.

"This use of a modified Fendr, also known as ExMatter, represents a new data point connecting BlackCat with past BlackMatter activity," the researchers said.

"The modification of this reused tool demonstrates a more sophisticated planning and development regimen for adapting requirements to target environments, characteristic of a maturing criminal enterprise."

SHARE □ □ □ □ □

SHARE □