Looking Into the Void: Probing a Top Bulletproof Hosting Service

trendmicro.com/vinfo/no/security/news/cybercrime-and-digital-threats/looking-into-the-void-probing-a-top-bulletproof-hosting-service

Looking Into the Void

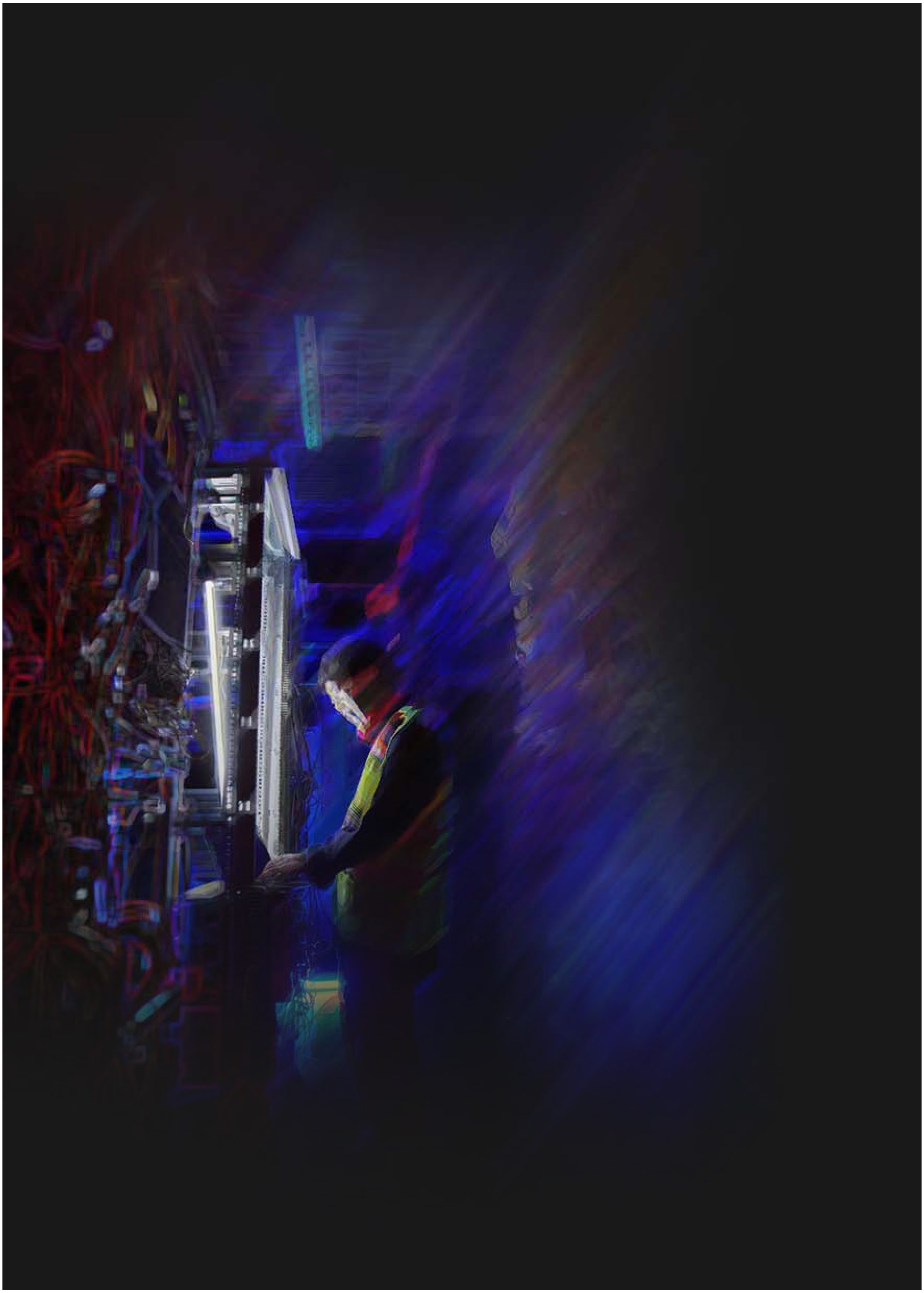
Targeting Bulletproof Hosts to Block Attacks Early in the Kill Chain

Bulletproof hosting providers are a key enabler of cybercrime operations and APT groups because they supply a stable infrastructure. Our investigation shows how the provider Void Griffon has been integral to the activities of a number of high-profile gangs.

One of the basic requirements to keeping a cybercriminal operation running smoothly, covertly, and for a prolonged period is a reliable web hosting service that can withstand abuse complaints and law enforcement takedown requests. These bulletproof hosting services are essentially cybercriminal hideouts for lease, designed specifically to give threat actors stable servers where they can store malicious files or even the malware necessary for their operations.

Void Griffon is our name for a provider that has been active since 2006. Its service has been used for multiple years by some of today's top-tier advanced persistent threat (APT) groups and malware distributors.

Trend Micro uses cybercriminals’ dependence on such infrastructure against them, tracking and proactively blocking such service providers to protect customers early in the attack chain. The short video series below tells you all you need to know about these bulletproof hosting service providers.



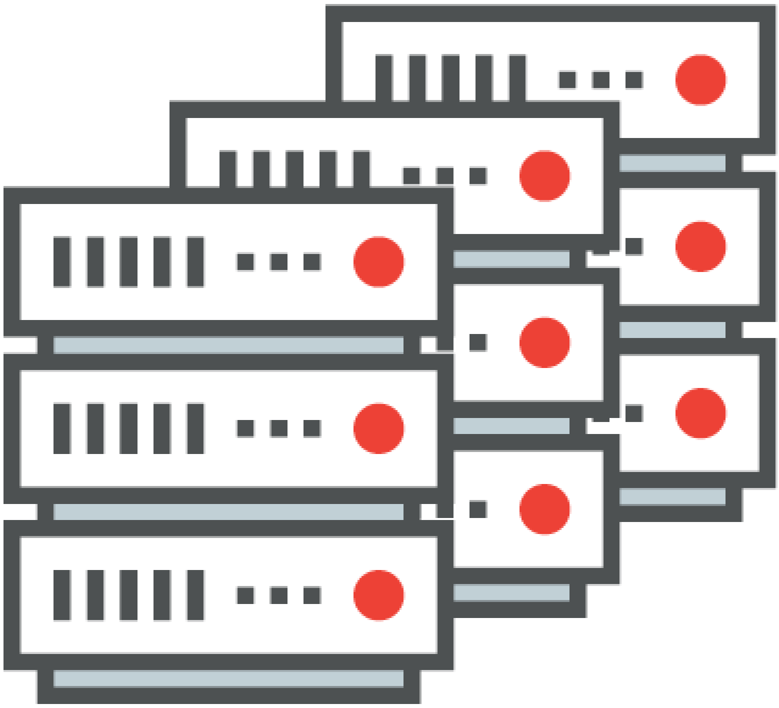
Digging into Void Griffon

Our investigation into one specific bulletproof hosting provider, which we track as Void Griffon, shows the exact services available, and how bulletproof hosting businesses support long-running cybercriminal operations.

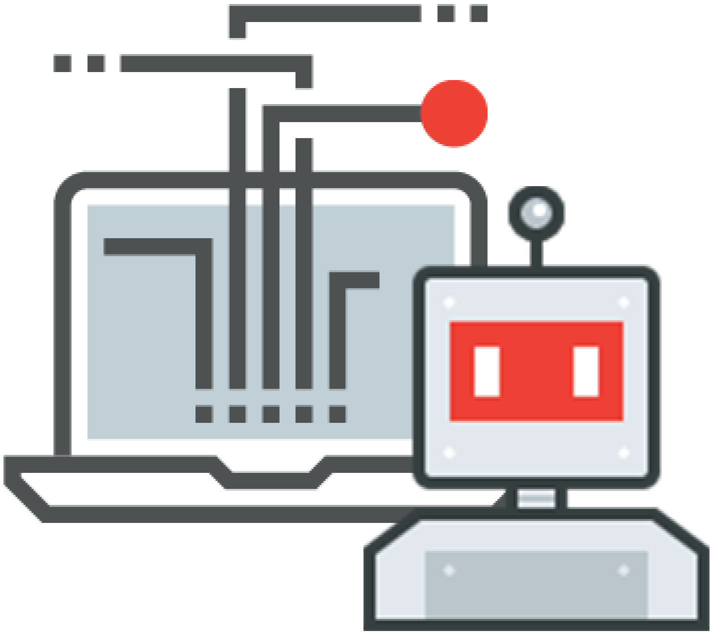
Void Griffon is a malicious actor group that we have been aware of since 2006. The group has had different aliases over the years and has advertised a slew of services in underground forums. It first offered its fast-flux bulletproof hosting service in 2015, and its business has since flourished. We have found that Void Griffon has been used by different APT groups and has also hosted many prominent malware families.

Services offered by Void Griffon

- Hosting

- 

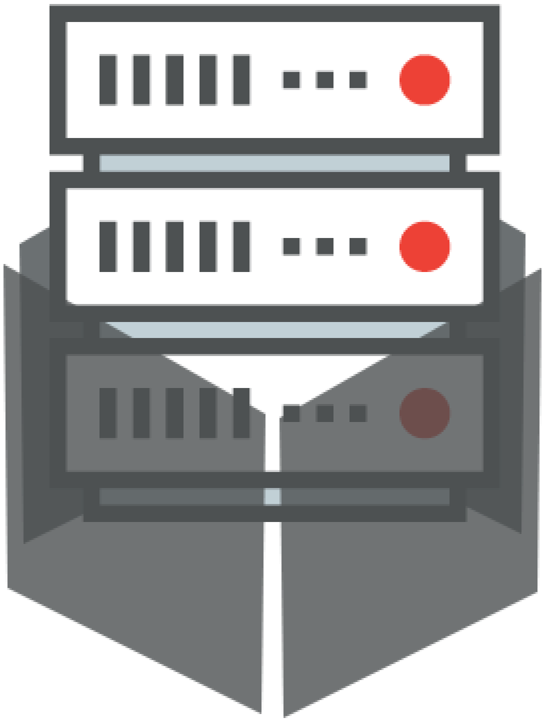
  Dedicated servers

- 

Node-based FastFlux, a shifting network for botnets

-

  Virtual private servers (VPSs)

- 

  Virtual dedicated servers (VDSs)

- Domain name registration

- API access

We can link the longevity and success of campaigns that use the malware families listed in Figure 1 to the affordable and stable hosting services made available by providers like Void Griffon. It is clear from the high-profile families on the list and the number of days they have been hosted on Void Griffon that the service has a good reputation. It is an important element that allows many cybercriminal operations to keep running smoothly.

Gandcrab	401
Razy	426
Redline Stealer	610

RacoonStealer

646

KPOT Stealer

663

Negasteal

691

Powload

727

Azorult

743

TinyNuke Bot

863

ClipBanker

873

Matrix

887

STOP Ransomware

935

Ramnit

1,029

Vidar

1,033

Dridex

1,064

Smoke Loader

	1,066
Lokibot	1,198
Fareit	1,246
Hancitor	1,442
Ursnif	1,729

Figure 1. The top 20 malware families in terms of the number of days they have been hosted by Void Griffon (based on data collected from February 2017 to March 2022)

Dismantling support systems

Malicious actors and high-profile malware are usually widely reported on, but security teams and law enforcement should also identify and disrupt the support systems that allow cybercriminal activities to thrive. Analyzing these systems by proactively locating and blocking the bulletproof hosting infrastructure will aid defenders in blocking attacks in the early stages of the kill chain.

However, this is difficult for a network defender to do on their own. Trend Micro’s threat intelligence allows us to do this on behalf of our customers and provide this protection directly in our products.

We hope to bring more attention to the support pillars that allow cybercriminal campaigns to operate, and what can be done to counteract them. Watch the short video series below for more details about Void Griffon.

Void Griffon:

Targeting Cybercriminals' Support System

[Watch Video At:](https://youtu.be/IFErUCkcjSY)

https://youtu.be/IFErUCkcjSY

Bulletproof hosting providers are key enablers of cybercriminal operations and advanced persistent threat (APT) groups. Our investigation shows how one such provider, Void Griffon, has been integral to the activities of a number of high-profile gangs.

HIDE

Like it? Add this infographic to your site:
1. Click on the box below.   2. Press Ctrl+A to select all.   3. Press Ctrl+C to copy.   4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

Posted in Cybercrime & Digital Threats, Cybercrime, Cybercriminal Underground