Feb 28 2024

NETMANAGEIT

Intelligence Report

StopRansomware: Blackcat

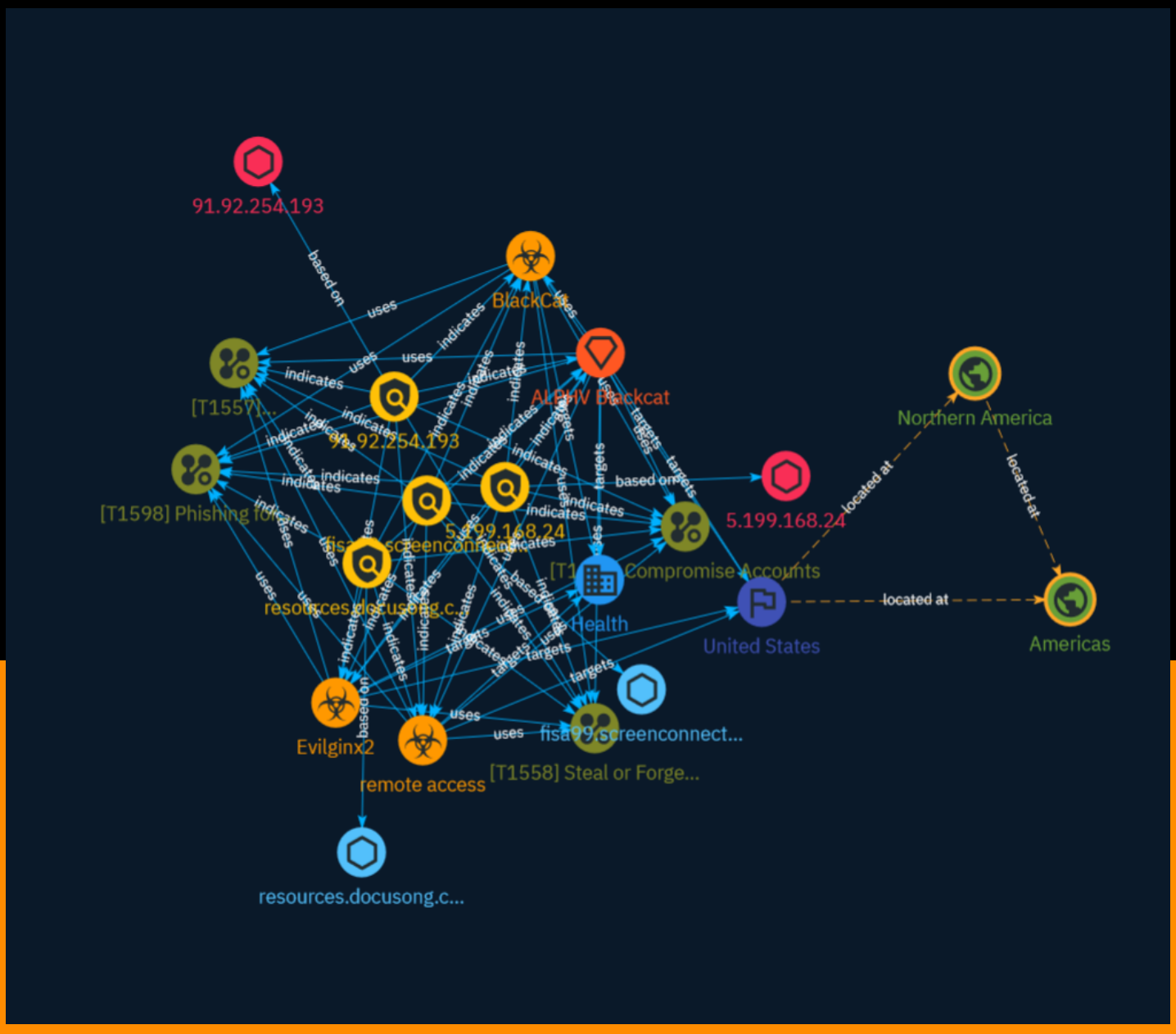

Table of contents

Overview

Entities

Observables

External References

Overview

Description

In February 2023, ALPHV Blackcat administrators announced the ALPHV Blackcat Ransomware 2.0 Sphynx update, which was rewritten to provide additional features to affiliates, such as better defense evasion and additional tooling. This ALPHV Blackcat update has the capability to encrypt both Windows and Linux devices, and VMWare instances. ALPHV Blackcat affiliates have extensive networks and experience with ransomware and data extortion operations.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Indicator

Name
fisa99.screenconnect.com
Pattern Type
stix
Pattern
[hostname:value = 'fisa99.screenconnect.com']
Name
resources.docusong.com
Pattern Type
stix
Pattern
[hostname:value = 'resources.docusong.com']
Name
91.92.254.193

Description
CC=BG ASN=AS394711 LIMENET
Pattern Type
stix
Pattern
[ipv4-addr:value = '91.92.254.193']
Name
5.199.168.24
Description
IcedID botnet C2 server (confidence level: 75%)
Pattern Type
stix
Pattern
[ipv4-addr:value = '5.199.168.24']

Malware

Name
Evilginx2
Name
remote access
Name
BlackCat
Description
[BlackCat](https://attack.mitre.org/software/S1068) is ransomware written in Rust that has been offered via the Ransomware-as-a-Service (RaaS) model. First observed November 2021, [BlackCat](https://attack.mitre.org/software/S1068) has been used to target multiple sectors and organizations in various countries and regions in Africa, the Americas, Asia, Australia, and Europe.(Citation: Microsoft BlackCat Jun 2022)(Citation: Sophos BlackCat Jul 2022)(Citation: ACSC BlackCat Apr 2022)

Intrusion-Set

Name
ALPHV Blackcat

Attack-Pattern

Name
Phishing for Information
ID
T1598
Description
Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information. Phishing for information is different from [Phishing](https://attack.mitre.org/techniques/T1566) in that the objective is gathering data from the victim rather than executing malicious code. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass credential harvesting campaigns. Adversaries may also try to obtain information directly through the exchange of emails, instant messages, or other electronic conversation means.(Citation: ThreatPost Social Media Phishing)(Citation: TrendMictro Phishing)(Citation: PCMag FakeLogin)(Citation: Sophos Attachment)(Citation: GitHub Phishery) Victims may also receive phishing messages that direct them to call a phone number where the adversary attempts to collect confidential information.(Citation: Avertium callback phishing) Phishing for information frequently involves social engineering techniques, such as posing as a source with a reason to collect information (ex: [Establish Accounts](https://attack.mitre.org/techniques/T1585) or [Compromise Accounts](https://attack.mitre.org/techniques/T1586)) and/or sending multiple, seemingly urgent messages. Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce)

Phishing for information may also involve evasive techniques, such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)). (Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014)

Name

Compromise Accounts

ID

T1586

Description

Adversaries may compromise accounts with services that can be used during targeting. For operations incorporating social engineering, the utilization of an online persona may be important. Rather than creating and cultivating accounts (i.e. [Establish Accounts](https://attack.mitre.org/techniques/T1585)), adversaries may compromise existing accounts. Utilizing an existing persona may engender a level of trust in a potential victim if they have a relationship, or knowledge of, the compromised persona. A variety of methods exist for compromising accounts, such as gathering credentials via [Phishing for Information](https://attack.mitre.org/techniques/T1598), purchasing credentials from third-party sites, brute forcing credentials (ex: password reuse from breach credential dumps), or paying employees, suppliers or business partners for access to credentials.(Citation: AnonHBGary) (Citation: Microsoft DEV-0537) Prior to compromising accounts, adversaries may conduct Reconnaissance to inform decisions about which accounts to compromise to further their operation. Personas may exist on a single site or across multiple sites (ex: Facebook, LinkedIn, Twitter, Google, etc.). Compromised accounts may require additional development, this could include filling out or modifying profile information, further developing social networks, or incorporating photos. Adversaries may directly leverage compromised email accounts for [Phishing for Information](https://attack.mitre.org/techniques/T1598) or [Phishing](https://attack.mitre.org/techniques/T1566).

Name

Steal or Forge Kerberos Tickets

ID

T1558

Description

Adversaries may attempt to subvert Kerberos authentication by stealing or forging Kerberos tickets to enable [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003). Kerberos is an authentication protocol widely used in modern Windows domain environments. In Kerberos environments, referred to as “realms”, there are three basic participants: client, service, and Key Distribution Center (KDC).(Citation: ADSecurity Kerberos Ring Decoder) Clients request access to a service and through the exchange of Kerberos tickets, originating from KDC, they are granted access after having successfully authenticated. The KDC is responsible for both authentication and ticket granting. Adversaries may attempt to abuse Kerberos by stealing tickets or forging tickets to enable unauthorized access. On Windows, the built-in `klist` utility can be used to list and analyze cached Kerberos tickets.(Citation: Microsoft Klist) Linux systems on Active Directory domains store Kerberos credentials locally in the credential cache file referred to as the "ccache". The credentials are stored in the ccache file while they remain valid and generally while a user's session lasts.(Citation: MIT ccache) On modern Redhat Enterprise Linux systems, and derivative distributions, the System Security Services Daemon (SSSD) handles Kerberos tickets. By default SSSD maintains a copy of the ticket database that can be found in `/var/lib/sss/secrets/secrets.ldb` as well as the corresponding key located in `/var/lib/sss/secrets/.secrets.mkey`. Both files require root access to read. If an adversary is able to access the database and key, the credential cache Kerberos blob can be extracted and converted into a usable Kerberos ccache file that adversaries may use for [Pass the Ticket](https://attack.mitre.org/techniques/T1550/003). The ccache file may also be converted into a Windows format using tools such as Kekeo.(Citation: Linux Kerberos Tickets)(Citation: Brining MimiKatz to Unix)(Citation: Kekeo) Kerberos tickets on macOS are stored in a standard ccache format, similar to Linux. By default, access to these ccache entries is federated through the KCM daemon process via the Mach RPC protocol, which uses the caller's environment to determine access. The storage location for these ccache entries is influenced by the `/etc/krb5.conf` configuration file and the `KRB5CCNAME` environment variable which can specify to save them to disk or keep them protected via the KCM daemon. Users can interact with ticket storage using `kinit`, `klist`, `ktutil`, and `kcc` built-in binaries or via Apple's native Kerberos framework. Adversaries can use open source tools to interact with the ccache files directly or to use the Kerberos framework to call lower-level APIs for extracting the user's TGT or Service Tickets.(Citation: SpectorOps Bifrost Kerberos macOS 2019)(Citation: macOS kerberos framework MIT)

Name

Adversary-in-the-Middle

ID

T1557

Description

Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as [Network Sniffing](https://attack.mitre.org/techniques/T1040), [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002), or replay attacks ([Exploitation for Credential Access](https://attack.mitre.org/techniques/T1212)). By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.(Citation: Rapid7 MiTM Basics) For example, adversaries may manipulate victim DNS settings to enable other malicious activities such as preventing/redirecting users from accessing legitimate sites and/or pushing additional malware.(Citation: ttint_rat)(Citation: dns_changer_trojans)(Citation: ad_blocker_with_miner) Adversaries may also manipulate DNS and leverage their position in order to intercept user credentials and session cookies. (Citation: volexity_0day_sophos_FW) [Downgrade Attack](https://attack.mitre.org/techniques/T1562/010)s can also be used to establish an AiTM position, such as by negotiating a less secure, deprecated, or weaker version of communication protocol (SSL/TLS) or encryption algorithm.(Citation: mitm_tls_downgrade_att)(Citation: taxonomy_downgrade_att_tls)(Citation: tlseminar_downgrade_att) Adversaries may also leverage the AiTM position to attempt to monitor and/or modify traffic, such as in [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002). Adversaries can setup a position similar to AiTM to prevent traffic from flowing to the appropriate destination, potentially to [Impair Defenses](https://attack.mitre.org/techniques/T1562) and/or in support of a [Network Denial of Service](https://attack.mitre.org/techniques/T1498).

Country

Name
United States

Region

Name
Northern America

Name
Americas

Sector

Name
Health
Description
Public and private entities involved in research, services and manufacturing activities related to public health.

Hostname

Value
fisa99.screenconnect.com
resources.docusong.com

IPv4-Addr

Value
91.92.254.193
5.199.168.24

External References

- https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-353a
- https://otx.alienvault.com/pulse/65df80858a3492ea38f98863