Apr 06 2024

NETMANAGEIT

Intelligence Report

Bing ad leads to SecTopRAT

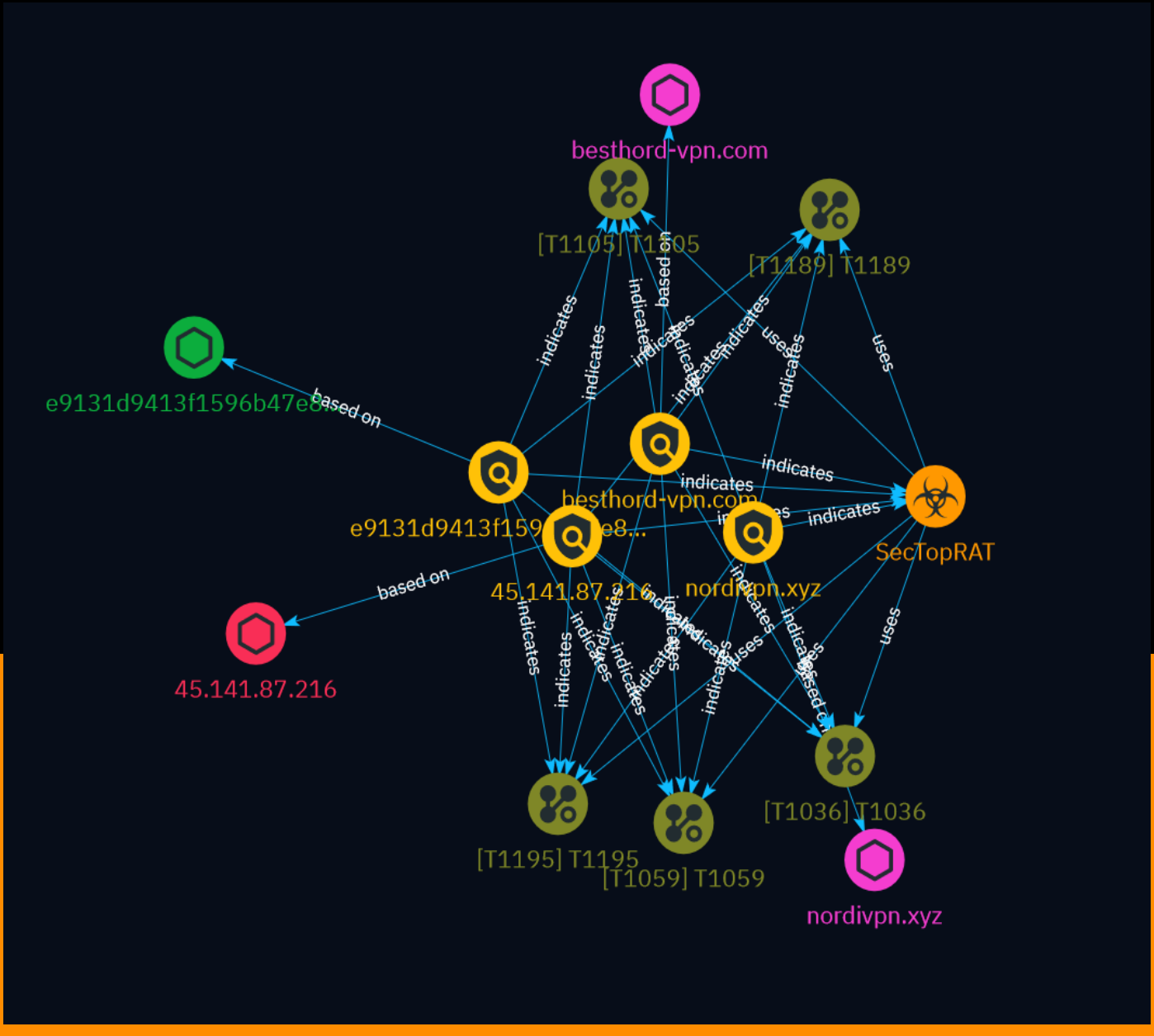

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This report details a recent malvertising campaign where threat actors abuse Microsoft Bing ads to impersonate the popular VPN provider NordVPN. Users searching for 'nord vpn' on Bing are shown a fraudulent ad that redirects them to a fake website mimicking NordVPN's official site. The website tricks victims into downloading a malicious installer posing as NordVPN's software, but also covertly installing the SecTopRAT remote access trojan on their systems. The report analyzes the traffic flow, malware payload, and provides indicators of compromise related to this campaign.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

nordivpn.xyz

Description

- **Unsafe:** True - **Server:** cloudflare - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '2 days ago', 'timestamp': 1712143110, 'iso': '2024-04-03T07:18:30-04:00'} - **IPQS: Domain:** nordivpn.xyz - **IPQS: IP Address:** 104.21.38.121

Pattern Type

stix

Pattern

[domain-name:value = 'nordivpn.xyz']

Name

besthord-vpn.com

Description

- **Unsafe:** True - **Server:** - **Domain Rank:** 0 - **DNS Valid:** True - **Parking:** False - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': '21 hours ago',

'timestamp': 1712239869, 'iso': '2024-04-04T10:11:09-04:00'} - **IPQS: Domain:** besthord-vpn.com - **IPQS: IP Address:** 62.113.104.190

Pattern Type

stix

Pattern

[domain-name:value = 'besthord-vpn.com']

Name

e9131d9413f1596b47e86e88dc5b4e4cc70a0a4ec2d39aa8f5a1a5698055adfc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e9131d9413f1596b47e86e88dc5b4e4cc70a0a4ec2d39aa8f5a1a5698055adfc']

Name

45.141.87.216

Description

ISP: Media Land LLC **OS:** Windows Server 2022 (build 10.0.20348) ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u3 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQC8DpUiSM5yBHrXa3Le+YKZPqMDi7dYM2wwa0W01HRx NsQZ X2AkvLn3+ +WQ8kCz0ajV8PQ0HRzyek8T+Pfaqw42SahiRKZY4lhYOAD7Vpm8OEIyHkyXK3z+xcht MPpGXKoXeAwr3CLO10qJjRlZ3voG2KZOCQj7ousF8khIf8kdrgf9N0VbKvLYk4Pmw4O9tjc44le5

37honmI40HfS62QSacqbzaV/AcuR9FieD8hQ4y1I4mSTepYDrE8y2siRgTVgHrDtF+X+12dSZ9gK Xp/ nSpQ6Tc7BATE4OzmR+YR5OCBY3FDJ9nifhDPpoSNRcQv27aapr9sacFQGnkLxNIDMNP0gC1Yw XYT1f6I1vk71HsBtm7XxKj18zVhG2hfotFDp3o2DaSykW8ZXfDsj4Cphp4xYLLROIwZbWLJweLbB I/ UEcMo9ptkcUgKRczOHmYYplnqYbiR4QtYh49lQ1RgjvACr1JuxskMcrkFkiXGqEaUwrOLpRzti vQNjTZRzZ3U= Fingerprint: da:f9:23:2c:4c:99:1e:e4:d8:16:ed:29:e8:11:64:d7 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 kex-strict-s-v00@openssh.com Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Thu, 28 Mar 2024 05:50:55 GMT Connection: close Content-Length: 315 WinRM NTLM Info: OS: Windows Server 2022 OS Build: 10.0.20348 Target Name: WIN-BFTHTH9I9PO NetBIOS Domain Name: WIN-BFTHTH9I9PO NetBIOS Computer Name: WIN-BFTHTH9I9PO DNS Domain Name: WIN-BFTHTH9I9PO FQDN: WIN-BFTHTH9I9PO ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.141.87.216']

Malware

Name
SecTopRAT

Attack-Pattern

Name
T1189
ID
T1189
Description
Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. With this technique, the user's web browser is typically targeted for exploitation, but adversaries may also use compromised websites for non-exploitation behavior such as acquiring [Application Access Token](https://attack.mitre.org/techniques/T1550/001). Multiple ways of delivering exploit code to a browser exist (i.e., [Drive-by Target](https://attack.mitre.org/techniques/T1608/004)), including: * A legitimate website is compromised where adversaries have injected some form of malicious code such as JavaScript, iFrames, and cross-site scripting * Script files served to a legitimate website from a publicly writeable cloud storage bucket are modified by an adversary * Malicious ads are paid for and served through legitimate ad providers (i.e., [Malvertising](https://attack.mitre.org/techniques/T1583/008)) * Built-in web application interfaces are leveraged for the insertion of any other kind of object that can be used to display web content or contain a script that executes on the visiting client (e.g. forum posts, comments, and other user controllable web content). Often the website used by an adversary is one visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is often referred to a strategic web compromise or watering hole attack. There are several known examples of this occurring.(Citation: Shadowserver Strategic Web Compromise) Typical drive-by compromise process: 1. A user visits a website that is used to host the adversary controlled content. 2. Scripts automatically execute, typically searching versions of the browser and plugins for a potentially vulnerable

version. * The user may be required to assist in this process by enabling scripting or active website components and ignoring warning dialog boxes. 3. Upon finding a vulnerable version, exploit code is delivered to the browser. 4. If exploitation is successful, then it will give the adversary code execution on the user's system unless other protections are in place. * In some cases a second visit to the website after the initial scan is required before exploit code is delivered. Unlike [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190), the focus of this technique is to exploit software on a client endpoint upon visiting a website. This will commonly give an adversary access to systems on the internal network instead of external systems that may be in a DMZ. Adversaries may also use compromised websites to deliver a user to a malicious application designed to [Steal Application Access Token](https://attack.mitre.org/techniques/T1528)s, like OAuth tokens, to gain access to protected applications and information. These malicious applications have been delivered through popups on legitimate websites.(Citation: Volexity OceanLotus Nov 2017)

Name

T1059

ID

T1059

Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote

Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

Name

T1105

ID

T1105

Description

Adversaries may transfer tools or other files from an external system into a compromised environment. Tools or files may be copied from an external adversary-controlled system to the victim network through the command and control channel or through alternate protocols such as [ftp](https://attack.mitre.org/software/S0095). Once present, adversaries may also transfer/spread tools between victim devices within a compromised environment (i.e. [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570)). On Windows, adversaries may use various utilities to download tools, such as `copy`, `finger`, [certutil](https://attack.mitre.org/software/S0160), and [PowerShell](https://attack.mitre.org/techniques/T1059/001) commands such as `IEX(New-Object Net.WebClient).downloadString()` and `Invoke-WebRequest`. On Linux and macOS systems, a variety of utilities also exist, such as `curl`, `scp`, `sftp`, `tftp`, `rsync`, `finger`, and `wget`. (Citation: t1105_lolbas) Adversaries may also abuse installers and package managers, such as `yum` or `winget`, to download tools to victim hosts. Files can also be transferred using various [Web Service](https://attack.mitre.org/techniques/T1102)s as well as native or otherwise present tools on the victim system.(Citation: PTSecurity Cobalt Dec 2016) In some cases, adversaries may be able to leverage services that sync between a web-based and an on-premises client, such as Dropbox or OneDrive, to transfer files onto victim systems. For example, by compromising a cloud account and logging into the service's web portal, an adversary may be able to trigger an automatic syncing process that transfers the file onto the victim's machine.(Citation: Dropbox Malware Sync)

Name

T1036

ID

T1036

Description

Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

Name

T1195

ID

T1195

Description

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise can take place at any stage of the supply chain including: * Manipulation of development tools * Manipulation of a development environment * Manipulation of source code repositories (public or private) * Manipulation of source code in open-source dependencies * Manipulation of software update/distribution mechanisms * Compromised/infected system images (multiple cases of removable media infected at the factory)(Citation: IBM Storwize)(Citation: Schneider Electric USB Malware) * Replacement of legitimate software with modified versions * Sales of modified/counterfeit products to legitimate distributors * Shipment interdiction While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update

channels.(Citation: Avast CCleaner3 2018)(Citation: Microsoft Dofoil 2018)(Citation: Command Five SK 2011) Targeting may be specific to a desired victim set or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Symantec Elderwood Sept 2012)(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011) Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency.(Citation: Trendmicro NPM Compromise)

Domain-Name

Value
besthord-vpn.com
nordivpn.xyz

StixFile

Value
e9131d9413f1596b47e86e88dc5b4e4cc70a0a4ec2d39aa8f5a1a5698055adfc

IPv4-Addr

Value
45.141.87.216

External References

- https://www.malwarebytes.com/blog/threat-intelligence/2024/04/bing-ad-for-nordvpn-leads-to-sectoprat
- https://otx.alienvault.com/pulse/660fdacee72f0bd4b501a0b7