Jun 10 2023

NETMANAGEIT

Intelligence Report

The distinctive rattle of APT SideWinder

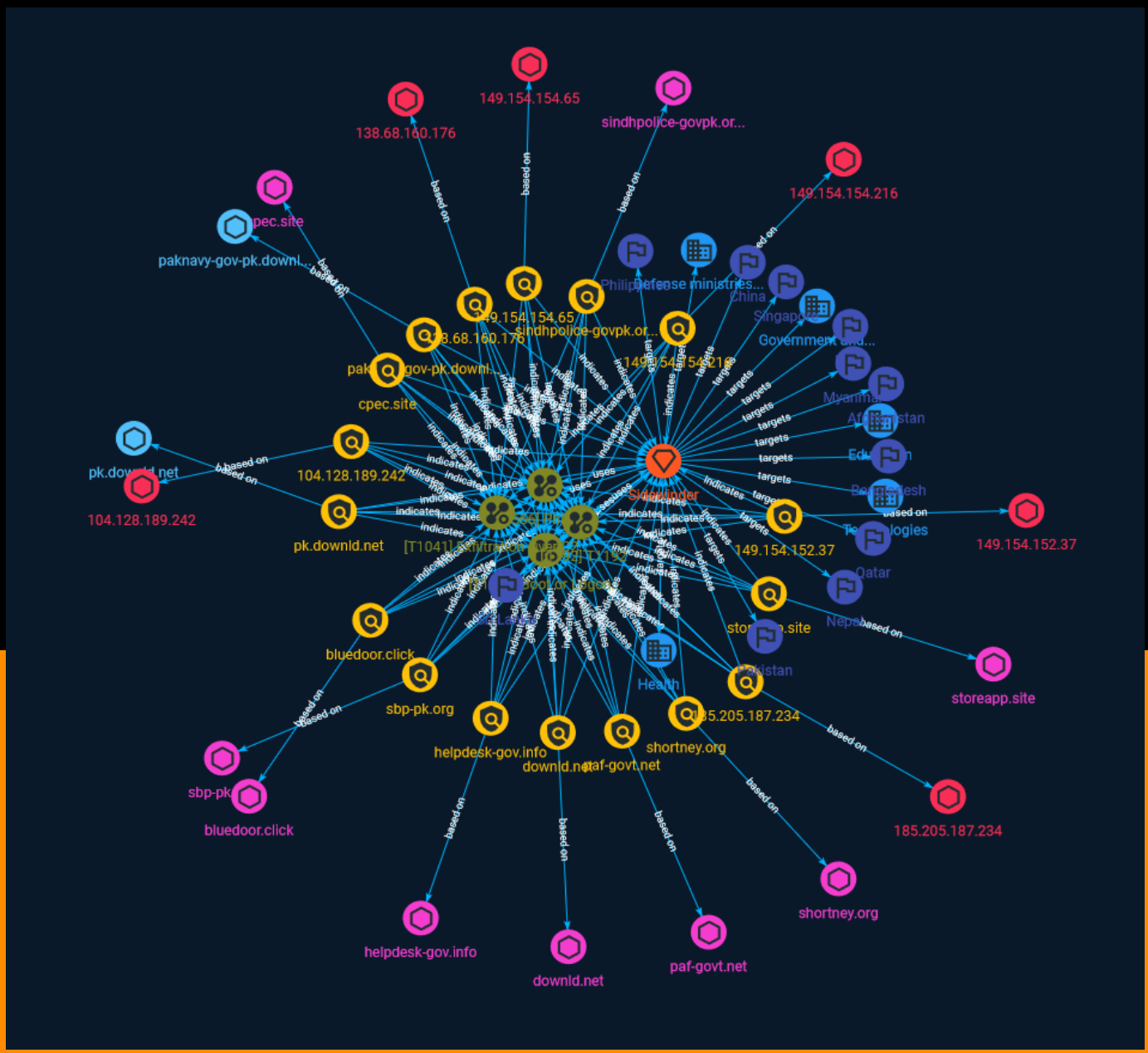

Table of contents

Overview

Entities

Observables

External References

Overview

Description

An analysis of SideWinder's network infrastructure

Confidence

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

15 / 100

Attack-Pattern

Name
Boot or Logon Autostart Execution
ID
T1547
Description
Adversaries may configure system settings to automatically execute a program during system boot or logon to maintain persistence or gain higher-level privileges on compromised systems. Operating systems may have mechanisms for automatically running a program on system boot or account logon.(Citation: Microsoft Run Key)(Citation: MSDN Authentication Packages)(Citation: Microsoft TimeProvider)(Citation: Cylance Reg Persistence Sept 2013)(Citation: Linux Kernel Programming) These mechanisms may include automatically executing programs that are placed in specially designated directories or are referenced by repositories that store configuration information, such as the Windows Registry. An adversary may achieve the same goal by modifying or extending features of the kernel. Since some boot or logon autostart programs run with higher privileges, an adversary may leverage these to elevate privileges.
Name
Phishing
ID
T1566

Description

Adversaries may send phishing messages to gain access to victim systems. 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 malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as 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) 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) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

T1192

ID

T1192

Name

Exfiltration Over C2 Channel

ID

T1041

Description

Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

Sector

Name
Defense ministries (including the military)
Description
Includes the military and all defense related-space activities.
Name
Education
Description
Public or private entities operating to facilitate learning and acquiring knowledge and skills, composed of infrastructures and services to host teachers, students, and administrative services related to this activity. This does not include research activities.
Name
Health
Description
Public and private entities involved in research, services and manufacturing activities related to public health.

Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.
Name
Technologies
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Indicator

Name
sindhpolice-govpk.org
Pattern Type
stix
Pattern
[domain-name:value = 'sindhpolice-govpk.org']
Name
downld.net
Pattern Type
stix
Pattern
[domain-name:value = 'downld.net']
Name
paknavy-gov-pk.downld.net

Pattern Type
stix
Pattern
[hostname:value = 'paknavy-gov-pk.downld.net']
Name
shortney.org
Pattern Type
stix
Pattern
[domain-name:value = 'shortney.org']
Name
bluedoor.click
Pattern Type
stix
Pattern
[domain-name:value = 'bluedoor.click']
Name
149.154.154.216

Description

ISP: EDIS GmbH **OS:** None ---------- Hostnames: - 216.154.154.149.in-addr.arpa - shortney.org ---------- Domains: - 149.in-addr.arpa - shortney.org ---------- Services: **443:** ``` HTTP/1.1 404 Not Found Server: nginx/1.23.2 Date: Wed, 19 Apr 2023 02:18:53 GMT Content-Type: text/html Content-Length: 555 Connection: keep-alive ``` HEARTBLEED: 2023/04/19 02:19:33 149.154.154.216:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '149.154.154.216']

Name

paf-govt.net

Pattern Type

stix

Pattern

[domain-name:value = 'paf-govt.net']

Name

104.128.189.242

Description

ISP: Nexeon Technologies, Inc. **OS:** None ---------- Hostnames: - cpec.site ---------- Domains: - cpec.site ---------- Services: **80:** ``` HTTP/

1.1 404 Not Found Server: nginx Date: Mon, 08 May 2023 07:13:34 GMT Content-Type: text/html Content-Length: 535 Connection: keep-alive ``` ---------- **443:** ``` HTTP/1.1 404 Not Found Server: nginx Date: Wed, 17 May 2023 00:51:38 GMT Content-Type: text/html Content-Length: 535 Connection: keep-alive ``` HEARTBLEED: 2023/05/17 00:51:45 104.128.189.242:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '104.128.189.242']

Name

149.154.152.37

Description

ISP: EDIS GmbH **OS:** Ubuntu ---------- Hostnames: - 37.152.154.149.in-addr.arpa ---------- Domains: - 149.in-addr.arpa ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQC/jy/goN1UJWkmJH4hQVitqPhsBSq55gbZUYZnc2kIgDGv cM73/F87E8+tVq6dm2L/CqAtMAjT2usgbE3vLY3N1v7mQgNHbX3wsoMG8ywDx7ldVGXPmh9xg323 fyxHlgUTjrrW7vCGNCvlA08EuODT1BrkDAkOcDCaIc+U5TJXd04njrEGWbyeyWnS6i3K4n8oyLaQ UI21eK/BFfTkI8eS89aAT1I+RrCehgXUhDLzx3N9kVu1H5zpHvCoups6vY3oSUYCjAnPy2VyAHsU 4NZ4tH55TdLYmNjWCxvWZF1mD5XTdlMCwCnpR0Mejof4HRaMvlYXKlJraUmykRI9N9x3YCgmtZNN 7kJV72VdvJd9OmnsvYkaO8Wu3TqyVR3I5AydJeamjhY/uvp1tW+zr6O672Rys/Bcd0O2u+u3bBHX SepnbziwyPjRMWTLHOQupMUyAJ4UXNJqmXBO0HNh0Ekw+OaLUkVgV2nr63mAMZGfkHsQ0fnOz0hG +nzbvVXG4vc= Fingerprint: ef:54:9a:a3:fe:71:9b:9b:aa:a3:e7:41:62:40:bd:4f 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 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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '149.154.152.37']

Name

sbp-pk.org

Pattern Type

stix

Pattern

[domain-name:value = 'sbp-pk.org']

Name

138.68.160.176

Description

ISP: DigitalOcean, LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 200 OK Date: Thu, 18 May 2023 08:28:16 GMT Server: Apache/2.4.41 (Ubuntu) Last-Modified: Thu, 01 Dec 2022 08:42:53 GMT ETag: "18-5eec035019b63" Accept-Ranges: bytes Content-Length: 24 Content-Type: text/html ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '138.68.160.176']

Name

185.205.187.234

Description

ISP: CLOUDLAYER8 LIMITED **OS:** None ---------- Hostnames: - hz08.superdesing.org - srv32953.yourbestnetwork.net ---------- Domains: - superdesing.org - yourbestnetwork.net ---------- Services: **25:** ``` 220 hz08.superdesing.org ESMTP service ready 250-hz08.superdesing.org says hello 250-ENHANCEDSTATUSCODES 250-PIPELINING 250-CHUNKING 250-8BITMIME 250-AUTH CRAM-MD5 250-AUTH=CRAM-MD5 250-XACK 250-SIZE 0 250-VERP 250 DSN ``` ---------- **80:** ``` HTTP/1.1 403 Forbidden Date: Tue, 09 May 2023 12:57:38 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_auth_kerb/5.4 mod_nss/1.0.14 NSS/3.28.4 PHP/5.4.16 SVN/1.7.14 mod_wsgi/3.4 Python/2.7.5 Last-Modified: Thu, 16 Oct 2014 13:20:58 GMT ETag: "1321-5058a1e728280" Accept-Ranges: bytes Content-Length: 4897 Content-Type: text/html; charset=UTF-8 ``` ---------- **443:** ``` HTTP/1.1 403 Forbidden Date: Wed, 26 Apr 2023 11:27:10 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_auth_kerb/5.4 mod_nss/1.0.14 NSS/3.28.4 PHP/5.4.16 SVN/1.7.14 mod_wsgi/3.4 Python/2.7.5 Last-Modified: Thu, 16 Oct 2014 13:20:58 GMT ETag: "1321-5058a1e728280" Accept-Ranges: bytes Content-Length: 4897 Content-Type: text/html; charset=UTF-8 ``` HEARTBLEED: 2023/04/26 11:27:39 185.205.187.234:443 - SAFE ---------- **8443:** ``` HTTP/1.1 403 Forbidden Date: Thu, 20 Apr 2023 03:13:15 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips mod_auth_kerb/5.4 mod_nss/1.0.14 NSS/3.28.4 PHP/5.4.16 SVN/1.7.14 mod_wsgi/3.4 Python/2.7.5 Last-Modified: Thu, 16 Oct 2014 13:20:58 GMT ETag: "1321-5058a1e728280" Accept-Ranges: bytes Content-Length: 4897 Content-Type: text/html; charset=UTF-8 ``` HEARTBLEED: 2023/04/20 03:13:23 185.205.187.234:8443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.205.187.234']

Name

pk.downld.net

Pattern Type

stix

Pattern

[hostname:value = 'pk.downld.net']

Name

149.154.154.65

Description

CC=AT ASN=AS57169 EDIS GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '149.154.154.65']

Name

helpdesk-gov.info

Pattern Type

stix

Pattern

[domain-name:value = 'helpdesk-gov.info']

Name

cpec.site

Pattern Type

stix

Pattern

[domain-name:value = 'cpec.site']

Name

storeapp.site

Pattern Type

stix

Pattern

[domain-name:value = 'storeapp.site']

Intrusion-Set

Name
Sidewinder

Description
[Sidewinder](https://attack.mitre.org/groups/G0121) is a suspected Indian threat actor group that has been active since at least 2012. They have been observed targeting government, military, and business entities throughout Asia, primarily focusing on Pakistan, China, Nepal, and Afghanistan.(Citation: ATT Sidewinder January 2021)(Citation: Securelist APT Trends April 2018)(Citation: Cyble Sidewinder September 2020)

Country

Name
India
Name
Qatar
Name
Philippines
Name
Afghanistan
Name
Pakistan
Name
Singapore
Name
Bangladesh

Name
Sri Lanka
Name
Myanmar
Name
Nepal
Name
China

Domain-Name

Value
storeapp.site
sbp-pk.org
downld.net
sindhpolice-govpk.org
paf-govt.net
cpec.site
helpdesk-gov.info
bluedoor.click
shortney.org

Hostname

Value
pk.downld.net
paknavy-gov-pk.downld.net

IPv4-Addr

Value
104.128.189.242
149.154.154.216
138.68.160.176
185.205.187.234
149.154.152.37
149.154.154.65

External References

- https://otx.alienvault.com/pulse/64662e42892932585c023e3a
- https://www.group-ib.com/blog/hunting-sidewinder/