Jul 04 2023

NETMANAGEIT

Intelligence Report

Technical Analysis of Bandit Stealer

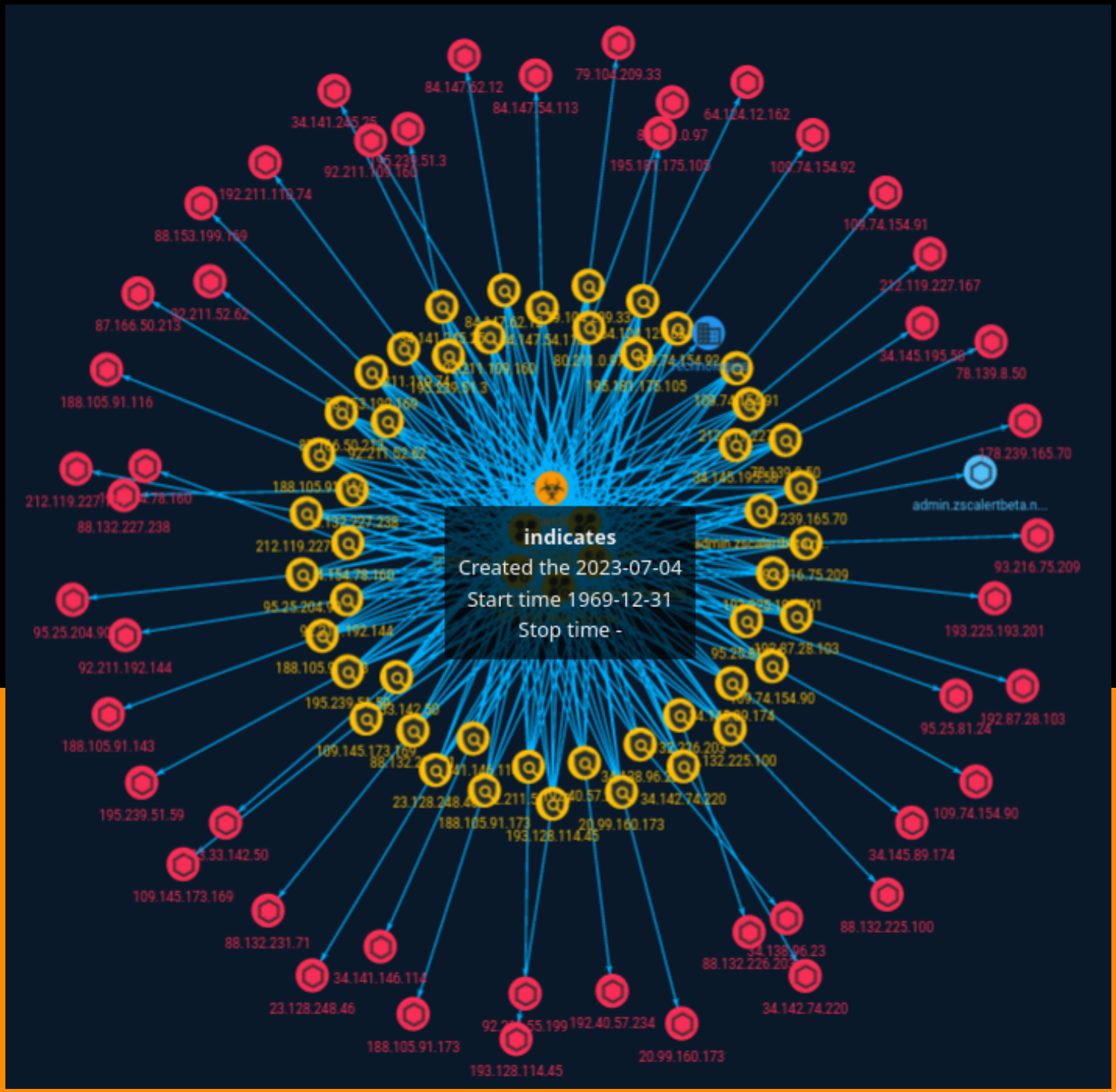

Table of contents

Overview

- Description 4
- Confidence 4

Entities

- Attack-Pattern 5
- Indicator 6
- Malware 30

Observables

- Hostname 31
- IPv4-Addr 32

External References

- External References 35

Overview

Description

Bandit is a new information stealer that harvests stored credentials from web browsers, FTP clients, email clients, and targets cryptocurrency wallet applications.

Confidence

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

15 / 100

Attack-Pattern

Name
T1214
ID
T1214

Indicator

Name

195.239.51.3

Description

ISP: PJSC "Vimpelcom" **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **1900:** ``` HTTP/1.1 200 OK CACHE-CONTROL: max-age=120 ST: upnp:rootdevice USN: uuid:007fd6fb-addc-3279-2152-62929b9a0878::upnp:rootdevice EXT: SERVER: ZyXEL Communications Corp. UPnP/1.0 MiniUPnPd/1.4 LOCATION: http://192.168.1.1:36533/rootDesc.xml UPnP Device: Device Type: urn:schemas-upnp-org:device:InternetGatewayDevice:1 Friendly Name: ZyXEL Keenetic Model Name: ZyXEL Keenetic Model Number: 020-763-363-750-434 Model Description: ZyXEL Keenetic Model URL: http://www.zyxel.ru/keenetic Manufacturer: ZyXEL Communications Corp. Manufacturer URL: http://www.zyxel.ru Serial Number: S120F19005841 UDN: uuid:007fd6fb-addc-3279-2152-62929b9a0878 Presentation URL: http://192.168.1.1 Sub Device #1: Device Type: urn:schemas-upnp-org:device:WANDevice:1 Friendly Name: WANDevice Model Name: WAN Device Model Number: ZyXEL Keenetic Model Description: WAN Device Model URL: http://www.zyxel.ru/keenetic Manufacturer: ZyXEL Communications Corp. Manufacturer URL: http://www.zyxel.ru Serial Number: S120F19005841 UDN: uuid:007fd6fb-addc-3279-2152-62929b9a0878 UPC: MINIUPNPD Sub Device #1: Device Type: urn:schemas-upnp-org:device:WANConnectionDevice:1 Friendly Name: WANConnectionDevice Model Name: ZyXEL Keenetic Model Number: ZyXEL Keenetic Model Description: ZyXEL Keenetic Model URL: http://www.zyxel.ru/keenetic Manufacturer: ZyXEL Communications Corp. Manufacturer URL: http://www.zyxel.ru Serial Number: S120F19005841 UDN: uuid:007fd6fb-addc-3279-2152-62929b9a0878 UPC: MINIUPNPD Service #1: Service Type: urn:schemas-upnp-org:service:WANIPConnection:1 Service ID: urn:upnp-org:serviceId:WANIPConn1 SCPD URL: /WANIPCn.xml Control URL: /ctl/IPConn Event Sub URL: /evt/IPConn Service #1: Service Type: urn:schemas-upnp-org:service:WANCommonInterfaceConfig:1 Service ID: urn:upnp-org:serviceId:WANCommonIFC1 SCPD URL: /WANCfg.xml Control URL: /ctl/CmnIfCfg Event Sub URL: /evt/CmnIfCfg Service #1: Service Type: urn:schemas-upnp-

org:service:Layer3Forwarding:1 Service ID: urn:upnp-org:serviceId:Layer3Forwarding1 SCPD URL: /L3F.xml Control URL: /ctl/L3F Event Sub URL: /evt/L3F ``` ---------- **36533:** ``` HTTP/1.1 404 Not Found Content-Type: text/html Connection: close Content-Length: 134 Server: ZyXEL Communications Corp. UPnP/1.0 MiniUPnPd/1.4 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.239.51.3']

Name

88.132.226.203

Description

CC=HU ASN=AS50181 KabelszatNet-2002. Musoreloszto es Kereskedelmi Kft.

Pattern Type

stix

Pattern

[ipv4-addr:value = '88.132.226.203']

Name

84.147.54.113

Description

CC=DE ASN=AS3320 Deutsche Telekom AG

Pattern Type
stix
Pattern
[ipv4-addr:value = '84.147.54.113']
Name
80.211.0.97
Description
CC=IT ASN=AS31034 Aruba S.p.A.
Pattern Type
stix
Pattern
[ipv4-addr:value = '80.211.0.97']
Name
34.138.96.23
Description
CC=US ASN=AS396982 GOOGLE-CLOUD-PLATFORM
Pattern Type
stix

Pattern

[ipv4-addr:value = '34.138.96.23']

Name

88.132.227.238

Description

ISP: KabelszatNet-2002. Musoreloszto es Kereskedelmi Kft. **OS:** None ---------- Hostnames: - host-88-132-227-238.kabelszat2002.hu ---------- Domains: - kabelszat2002.hu ---------- Services: **443:** ``` HTTP/1.1 200 OK Cache-Control: max-age=31536000 Connection: Keep-Alive Content-Length: 5193 Content-Type: text/html Date: Tue, 27 Jun 2023 13:37:15 GMT Expires: Wed, 26 Jun 2024 13:37:15 GMT X-Frame-Options: sameorigin ``` HEARTBLEED: 2023/06/27 13:37:49 88.132.227.238:443 - SAFE ---------- **1701:** ``` \xc8\x02\x00g\x00\x00\x00\x00\x00\x00\x00\x01\x80\x08\x00\x00\x00\x00\x00\x02\ x80\x08\x00\x00\x00\x02\x01\x00\x80\n\x00\x00\x00\x03\x00\x00\x00\x01\x80\n\x00 \x00\x00\x04\x00\x00\x00\x00\x00\x08\x00\x00\x00\x06\x00\x01\x80\x11\x00\x00\x0 0\x07kajakhaz_gw\x00\x0e\x00\x00\x00\x08MikroTik\x80\x08\x00\x00\x00\t\x00*\x80\ x08\x00\x00\x00\n\x00\x04 ``` ---------- **1723:** ``` PPTP: Firmware: 1 Hostname: kajakhaz_gw Vendor: MikroTik ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '88.132.227.238']

Name

193.225.193.201

Description

CC=HU ASN=AS1955 KIFU (Governmental Info Tech Development Agency)

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.225.193.201']

Name

188.105.91.143

Description

CC=DE ASN=AS3209 Vodafone GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '188.105.91.143']

Name

84.147.62.12

Description

CC=DE ASN=AS3320 Deutsche Telekom AG

Pattern Type

stix

Pattern

[ipv4-addr:value = '84.147.62.12']

Name

88.132.225.100

Description

CC=HU ASN=AS50181 KabelszatNet-2002. Musoreloszto es Kereskedelmi Kft.

Pattern Type

stix

Pattern

[ipv4-addr:value = '88.132.225.100']

Name

212.119.227.151

Description

CC=RU ASN=AS3216 PVimpelCom

Pattern Type

stix

Pattern

[ipv4-addr:value = '212.119.227.151']

Name

195.181.175.105

Description

CC=CZ ASN=AS60068 Datacamp Limited

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.181.175.105']

Name

34.141.146.114

Description

CC=NL ASN=AS396982 GOOGLE-CLOUD-PLATFORM

Pattern Type

stix

Pattern

[ipv4-addr:value = '34.141.146.114']

Name

92.211.52.62

Description

CC=DE ASN=AS3209 Vodafone GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '92.211.52.62']

Name

95.25.81.24

Description

CC=RU ASN=AS42110 PVimpelCom

Pattern Type

stix

Pattern

[ipv4-addr:value = '95.25.81.24']

Name

194.154.78.160

Description

CC=RU ASN=AS3216 PVimpelCom

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.154.78.160']

Name

109.74.154.92

Description

CC=SK ASN=AS29405 VNET a.s.

Pattern Type

stix

Pattern

[ipv4-addr:value = '109.74.154.92']

Name

92.211.55.199

Description

CC=DE ASN=AS3209 Vodafone GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '92.211.55.199']

Name

192.211.110.74

Description

CC=US ASN=AS721 DNIC-ASBLK-00721-00726

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.211.110.74']

Name

192.87.28.103

Description

CC=NL ASN=AS1103 SURF B.V.

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.87.28.103']

Name

88.132.231.71

Description

CC=HU ASN=AS50181 KabelszatNet-2002. Musoreloszto es Kereskedelmi Kft.

Pattern Type

stix

Pattern

[ipv4-addr:value = '88.132.231.71']

Name

64.124.12.162

Description

CC=US ASN=AS6461 ZAYO-6461

Pattern Type

stix

Pattern

[ipv4-addr:value = '64.124.12.162']

Name

193.128.114.45

Description

CC=GB ASN=AS702 UUNET

Pattern Type

stix

Pattern

[ipv4-addr:value = '193.128.114.45']

Name

188.105.91.116

Description

CC=DE ASN=AS3209 Vodafone GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '188.105.91.116']

Name

34.145.195.58

Description

CC=US ASN=AS396982 GOOGLE-CLOUD-PLATFORM

Pattern Type

stix

Pattern

[ipv4-addr:value = '34.145.195.58']

Name

192.40.57.234

Description

CC=NL ASN=AS46562 PERFORMIVE

Pattern Type

stix

Pattern

[ipv4-addr:value = '192.40.57.234']

Name

92.211.109.160

Description

CC=DE ASN=AS3209 Vodafone GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '92.211.109.160']

Name

109.74.154.90

Description

CC=SK ASN=AS29405 VNET a.s.

Pattern Type

stix

Pattern

[ipv4-addr:value = '109.74.154.90']

Name

213.33.142.50

Description

ISP: PJSC "Vimpelcom" **OS:** None ---------- Hostnames: - mail.areal-hotel.ru ---------- Domains: - areal-hotel.ru ---------- Services: **1701:** ```
\xc8\x02\x00E\x00\x00\x00\x00\x00\x00\x00\x01\x80\x08\x00\x00\x00\x00\x00\x04\
x80\x08\x00\x00\x00\t1k\x80)\x00\x00\x00\x01\x00\x02\x00\x06Missing your assigned tunnel ID ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '213.33.142.50']

Name

212.119.227.167

Description

ISP: PJSC "Vimpelcom" **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **23:** ``` User Access Verification Username: ``` HEARTBLEED: 2023/06/23 09:29:52 212.119.227.167:23 - ERROR: tls: oversized record received with length 65531 ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '212.119.227.167']

Name

34.145.89.174

Description

CC=US ASN=AS396982 GOOGLE-CLOUD-PLATFORM

Pattern Type
stix

Pattern
[ipv4-addr:value = '34.145.89.174']

Name
87.166.50.213

Description
ISP: Deutsche Telekom AG **OS:** None ------------------------- Hostnames: - p57a632d5.dip0.t-ipconnect.de ------------------------- Domains: - t-ipconnect.de ------------------------- Services: **8089:** ``` HTTP/1.1 404 Not Found Content-Length: 0 ``` ----------

Pattern Type
stix

Pattern
[ipv4-addr:value = '87.166.50.213']

Name
78.139.8.50

Description
CC=HU ASN=AS21334 Vodafone Hungary Ltd.

Pattern Type

stix

Pattern

[ipv4-addr:value = '78.139.8.50']

Name

109.145.173.169

Description

ISP: British Telecommunications PLC **OS:** None ---------- Hostnames: - host109-145-173-169.range109-145.btcentralplus.com ---------- Domains: - btcentralplus.com ---------- Services: **7547:** ``` HTTP/1.1 404 Not Found Server: gSOAP/2.7 Content-Length: 0 Connection: close ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '109.145.173.169']

Name

79.104.209.33

Description

ISP: PJSC "Vimpelcom" **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **123:** ``` NTP version: 4 processor: unknown system: UNIX leap: 3 stratum: 16 precision: -28 rootdelay: 0.000

rootdispersion: 284978.384 peer: 0 refid: INIT reftime: 0x00000000.00000000 poll: 6 clock: 0xE83A109C.F168A0B2 state: 1 offset: 0.000 frequency: 0.000 jitter: 0.000 noise: 0.000 stability: 0.000 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '79.104.209.33']

Name

34.142.74.220

Description

CC=GB ASN=AS396982 GOOGLE-CLOUD-PLATFORM

Pattern Type

stix

Pattern

[ipv4-addr:value = '34.142.74.220']

Name

92.211.192.144

Description

CC=DE ASN=AS3209 Vodafone GmbH

Pattern Type
stix
Pattern
[ipv4-addr:value = '92.211.192.144']
Name
178.239.165.70
Description
CC=CH ASN=AS25369 Hydra Communications Ltd
Pattern Type
stix
Pattern
[ipv4-addr:value = '178.239.165.70']
Name
188.105.91.173
Description
CC=DE ASN=AS3209 Vodafone GmbH
Pattern Type
stix

Pattern

[ipv4-addr:value = '188.105.91.173']

Name

88.153.199.169

Description

CC=DE ASN=AS3209 Vodafone GmbH

Pattern Type

stix

Pattern

[ipv4-addr:value = '88.153.199.169']

Name

93.216.75.209

Description

ISP: Deutsche Telekom AG **OS:** None ---------- Hostnames: - abenteuerland.schulle-karlsruhe.de - p5dd84bd1.dip0.t-ipconnect.de - cloud.schulle-karlsruhe.de - traccar.schulle-karlsruhe.de - ibs.schulle-karlsruhe.de - www.schulle-karlsruhe.de - schulle-karlsruhe.de ---------- Domains: - t-ipconnect.de - schulle-karlsruhe.de ---------- Services: **80:** ``` HTTP/1.1 301 Moved Permanently Date: Thu, 29 Jun 2023 02:39:53 GMT Server: Apache/2.4.25 (Debian) OpenSSL/1.0.2u mod_perl/2.0.10 Perl/v5.24.1 Location: https://93.216.75.209 Content-Length: 229 Content-Type: text/html; charset=iso-8859-1 ``` ---------- **443:** ``` HTTP/1.1 200 OK Date: Thu, 29 Jun 2023 10:19:29 GMT Server: Jetty(9.4.12.v20180830) Last-Modified: Sun, 13 Jan 2019 21:11:32 GMT Content-Type: text/html Accept-Ranges: bytes Cache-Control: max-

age=3600,public Content-Length: 539 Vary: Accept-Encoding ``` HEARTBLEED: 2023/06/29 10:20:10 93.216.75.209:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '93.216.75.209']

Name

195.239.51.59

Description

CC=RU ASN=AS3216 PVimpelCom

Pattern Type

stix

Pattern

[ipv4-addr:value = '195.239.51.59']

Name

109.74.154.91

Description

CC=SK ASN=AS29405 VNET a.s.

Pattern Type
stix
Pattern
[ipv4-addr:value = '109.74.154.91']
Name
20.99.160.173
Description
CC=US ASN=AS8075 MICROSOFT-CORP-MSN-AS-BLOCK
Pattern Type
stix
Pattern
[ipv4-addr:value = '20.99.160.173']
Name
95.25.204.90
Description
CC=RU ASN=AS3216 PVimpelCom
Pattern Type
stix

Pattern

[ipv4-addr:value = '95.25.204.90']

Name

admin.zscalertbeta.net

Pattern Type

stix

Pattern

[hostname:value = 'admin.zscalertbeta.net']

Name

23.128.248.46

Description

CC=US ASN=AS55103 THIN-NOLOGY

Pattern Type

stix

Pattern

[ipv4-addr:value = '23.128.248.46']

Name

34.141.245.25

Description
CC=NL ASN=AS396982 GOOGLE-CLOUD-PLATFORM
Pattern Type
stix
Pattern
[ipv4-addr:value = '34.141.245.25']

Malware

Name
Bandit

Hostname

Value
admin.zscalertbeta.net

IPv4-Addr

Value
194.154.78.160
92.211.52.62
188.105.91.173
34.141.146.114
192.87.28.103
109.74.154.91
20.99.160.173
109.145.173.169
88.132.225.100
195.181.175.105
192.211.110.74
92.211.109.160
80.211.0.97

88.153.199.169
88.132.227.238
92.211.192.144
92.211.55.199
34.145.195.58
79.104.209.33
95.25.204.90
34.141.245.25
109.74.154.90
193.128.114.45
84.147.54.113
23.128.248.46
109.74.154.92
192.40.57.234
88.132.231.71
95.25.81.24
195.239.51.59
212.119.227.151

212.119.227.167
64.124.12.162
88.132.226.203
193.225.193.201
87.166.50.213
195.239.51.3
213.33.142.50
188.105.91.143
34.138.96.23
34.142.74.220
93.216.75.209
34.145.89.174
188.105.91.116
78.139.8.50
178.239.165.70
84.147.62.12

External References

- https://otx.alienvault.com/pulse/64a44720b5058955812bdc19
- https://www.zscaler.com/blogs/security-research/technical-analysis-bandit-stealer