Dec 12 2023

NETMANAGEIT

Intelligence Report

Sandman APT | China-Based Adversaries Embrace Lua

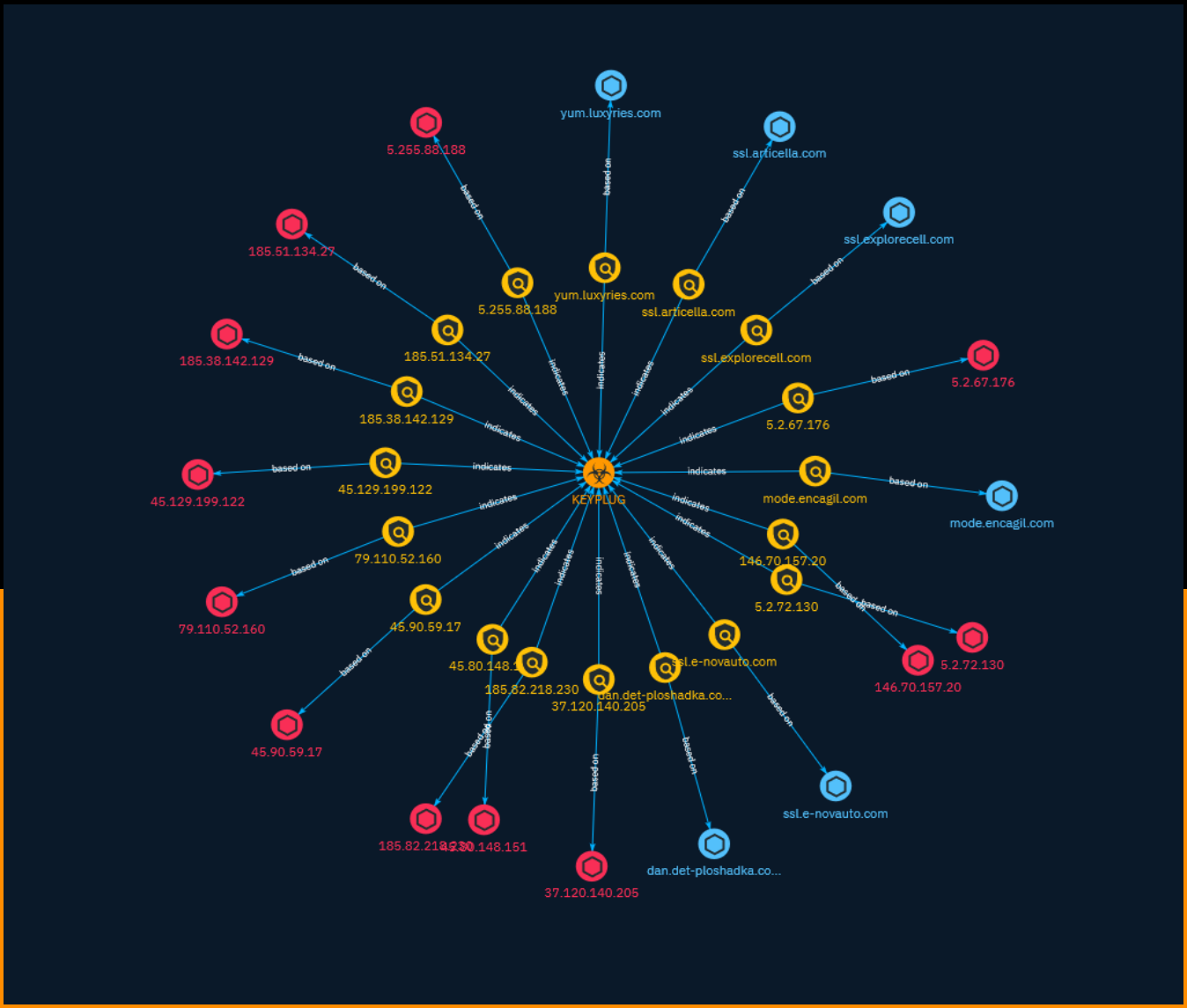

Table of contents

Overview

Entities

Observables

External References

Overview

Description

SentinelLabs, Microsoft, and PwC threat intelligence researchers provide attribution-relevant information on the Sandman APT cluster.

Confidence

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

15 / 100

Content

N/A

Indicator

Name
mode.encagil.com
Pattern Type
stix
Pattern
[hostname:value = 'mode.encagil.com']
Name
37.120.140.205
Pattern Type
stix
Pattern
[ipv4-addr:value = '37.120.140.205']
Name
185.51.134.27

Description

ISP: EstNOC OY **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_6.6.1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCrmRkvV5QPxOotk6upAUKDsHz+eH5JB0qu2MbimNw7tWho o+K9mgadtGiSmVoLniBUuLG0x4lJ7mYqYUSW3TlshPHPK1mancXpd7QgxM4FQcmjOUd2hwFmhA6r RiUk+ue/5b4FjJwZfZAzbefd9j3AhdEBtVCN91gT2a1rfuwaeUEmDXzLcv1k6/nHtzIbGI6yyWVR bg5PUAX+GSekAwXDXqciOiHhP4e5u0Z7biOcx3IsUI+axBdX44IcSntfg65Msp2UPadvRhWfrBS7GJ5xzqpl8khRs8Ti3mmrXsDhAqUdDpjDvHeidtXJohU9bPobdQOulXpkWjRA1QCPFpZT Fingerprint: 14:7d:e8:17:da:0c:08:72:cd:34:fc:27:f5:a8:46:d7 Kex Algorithms: curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: aes128-ctr aes192-ctr aes256-ctr arcfour256 arcfour128 aes128-gcm@openssh.com aes256-gcm@openssh.com chacha20-poly1305@openssh.com aes128-cbc 3des-cbc blowfish-cbc cast128-cbc aes192-cbc aes256-cbc arcfour rijndael-cbc@lysator.liu.se MAC Algorithms: hmac-md5-etm@openssh.com hmac-sha1-etm@openssh.com umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-ripemd160-etm@openssh.com hmac-sha1-96-etm@openssh.com hmac-md5-96-etm@openssh.com hmac-md5 hmac-sha1 umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-ripemd160 hmac-ripemd160@openssh.com hmac-sha1-96 hmac-md5-96 Compression Algorithms: none zlib@openssh.com ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.51.134.27']

Name

dan.det-ploshadka.com

Pattern Type
stix
Pattern
[hostname:value = 'dan.det-ploshadka.com']
Name
45.129.199.122
Pattern Type
stix
Pattern
[ipv4-addr:value = '45.129.199.122']
Name
yum.luxyries.com
Pattern Type
stix
Pattern
[hostname:value = 'yum.luxyries.com']
Name
5.2.72.130

Pattern Type
stix
Pattern
[ipv4-addr:value = '5.2.72.130']
Name
5.2.67.176
Pattern Type
stix
Pattern
[ipv4-addr:value = '5.2.67.176']
Name
ssl.e-novauto.com
Pattern Type
stix
Pattern
[hostname:value = 'ssl.e-novauto.com']
Name
45.80.148.151

Pattern Type
stix
Pattern
[ipv4-addr:value = '45.80.148.151']
Name
ssl.explorecell.com
Pattern Type
stix
Pattern
[hostname:value = 'ssl.explorecell.com']
Name
ssl.articella.com
Pattern Type
stix
Pattern
[hostname:value = 'ssl.articella.com']
Name
79.110.52.160

Description

ISP: M247 Europe SRL **OS:** None ------------------------- Hostnames: ------------------------- Domains: ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDKw5KpITV+/0PrQADwZIDcGUBx1kxwliikhg4UGSwa8we3 MeR/TMQwhhdPeRbr96ewIYz014PUosVbkdGQgd5OmlHZWxv/eRmnsySEnMRV8vLkzF2OnlqTbSxwYzl5bYjcjzcXKyJQ+DpbAyGAyQCXMCgcWYLjrJGhTmBn2dlPJTD8Lq+e+cRd2G9l8rEwzJmX5vgLl+WssPkvGb7SPbd/KKUvAH1igDdzp15v+AL1lNY7WTVw34JTAxccZTF7zftUmUBbzrhkN+yy/0G/FopKGfTDYOmaVVcPfEolMGfTaJobPFUA3bJ9PrinJwvM12ynH8r366KPd2Z1ePqfCnp5 Fingerprint: d4:0a:d1:3c:f3:bb:bb:b3:69:6a:a3:f3:66:27:cb:2f 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-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 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 aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc 3des-cbc 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 = '79.110.52.160']

Name

146.70.157.20

Description

ISP: M247 Europe SRL **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCqmiRIiqCBV7cMHJDc823/sVTbVLwb5VkZTMoC4YLXaxdf TSPZ0bkAZ71HtBexWgR4fYVhT2hQzTXIwgu6m3pl9OSTYcPFqf33rg5+aj3eeR9ETgeoOLiAFcTq 4Bt5SklgGtw4j9g1S6COUXUSKE4ek15GNgeNmFrjrBB0tMZjnHE8pdBWrBHC3x3KPnc5ybHsOPrX hdhvKZvRSYRuBCK19bK+YMY0nqfA4c80hVw8XrppXwSo23Lnk5fm6t2USgcU+L8Nqjj8Ggo3VGH w qEoTBnaqPuFPTM8XbWQwh3wqVtwHF7CfUFzg1w0flwZDMcsHs+vjZ08HhRafIuLNyuZx Fingerprint: 53:5b:6f:5f:07:b8:ea:32:61:d8:70:8e:6b:84:22:e9 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-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 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 aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc 3des-cbc 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 = '146.70.157.20']

Name

185.38.142.129

Description

ISP: Net Solutions - Consultoria Em Tecnologias De Informacao, Sociedade Unipessoal LDA **OS:** None ---------- Hostnames: - my.bllllla.xyz ---------- Domains: - bllllla.xyz ---------- Services: **22:** ```

SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDMDLshMj0BvHYbQ+tBYWU1nPPUOTZZhNc35dCU1mHylgma bOjdEXf/0rgVDnlsHAEPPKWR31IbEOevd8nYjYGvBrKZ9BQXO5BRRX523ysIn8XVkUN4CgYBRLCZ59aQtukV/QIlyjFTzJuZOpKG/y8hJFdOIRlQzePFswHSms8+mk+HFBnQAq0kQNBrM173pvk+2L6wuhXIAFeJZ4DtdqWxnAdpfYGgXv2yuLSY/LKvZy0JCjc7Y0Ah2YGCF8YwI/WzNaRg0aOT2qqdxidsGhDLIckw7ExXAdQ0ZxtOvucQ5ceyq6UFKuODptoDJfC99fydDLB3LJq9fARXfsTaCviL Fingerprint: dc:fe:31:2b:2f:bf:34:21:bd:8b:a8:d5:9a:28:a5:54 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-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 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 aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc 3des-cbc 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 ```
---------- **111:** ``` Portmap Program Version Protocol Port portmapper 4 tcp 111 portmapper 3 tcp 111 portmapper 2 tcp 111 portmapper 4 udp 111 portmapper 3 udp 111 portmapper 2 udp 111 ``` ---------- **111:** ``` Portmap Program Version Protocol Port portmapper 4 tcp 111 portmapper 3 tcp 111 portmapper 2 tcp 111 portmapper 4 udp 111 portmapper 3 udp 111 portmapper 2 udp 111 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.38.142.129']

Name

45.90.59.17

Description

ISP: GREEN FLOID LLC **OS:** None ---------- Hostnames: - dan.det-ploshadka.com - vds1166756.hosted-by-itldc.com ---------- Domains: - det-ploshadka.com - hosted-by-itldc.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQCw25AC+HeQLz1NdcKdKebfPJ7vBYBreRGAXL7tnrdxCpS54XD3KkVAFFQ+yKrSiwgb7AqbV4by7hxrsydyMu94Z8rmlkcSdbDv6nYYonxuLHfbQA+HCuYev7lZ1KXRT0jOj5ED/HRoh9ugaj3Cfj4WPGM3L7CSnJniN3y+Y/sb8MMbivtuolb18YNx4EtnTXSsps8j+GIVSqSop0CmsZ4U0dxmAoX2YhNfsOI+ns+nSfdvQjGJx/W+pE1Vfh22SeCnuD0kBGBJq4mIu74llDWpx5NCYDus4TK+u7su6wUZQXhC41qDT5LIYVS6vmHa28mCWhW4bqN1MQQ6SZqsp8LH Fingerprint: c3:3a:d7:37:22:ff:37:5b:53:91:d3:32:7b:d9:91:b6 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-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 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 aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc 3des-cbc 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 ``` ---------- **443:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Thu, 07 Dec 2023 04:31:44 GMT Connection: close Content-Length: 315 ``` HEARTBLEED: 2023/12/06 04:38:25 45.90.59.17:443 - SAFE ----------

Pattern Type
stix

Pattern
[ipv4-addr:value = '45.90.59.17']

Name
185.82.218.230

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.82.218.230']

Name

5.255.88.188

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.255.88.188']

Malware

Name
KEYPLUG

Description
[KEYPLUG](https://attack.mitre.org/software/S1051) is a modular backdoor written in C++, with Windows and Linux variants, that has been used by [APT41](https://attack.mitre.org/groups/G0096) since at least June 2021.(Citation: Mandiant APT41)

Hostname

Value
ssl.explorecell.com
dan.det-ploshadka.com
yum.luxyries.com
mode.encagil.com
ssl.e-novauto.com
ssl.articella.com

IPv4-Addr

Value
79.110.52.160
185.82.218.230
5.2.72.130
45.90.59.17
185.38.142.129
45.80.148.151
146.70.157.20
5.255.88.188
37.120.140.205
185.51.134.27
5.2.67.176
45.129.199.122

External References

- https://otx.alienvault.com/pulse/657880e45fb217d3766c1f55
- https://www.sentinelone.com/labs/sandman-apt-china-based-adversaries-embrace-lua/