Jun 11 2023

NETMANAGEIT

Intelligence Report

Ongoing MEME#4CHAN Attack/Phishing Campaign uses Meme-Filled Code to Drop XWorm Payloads

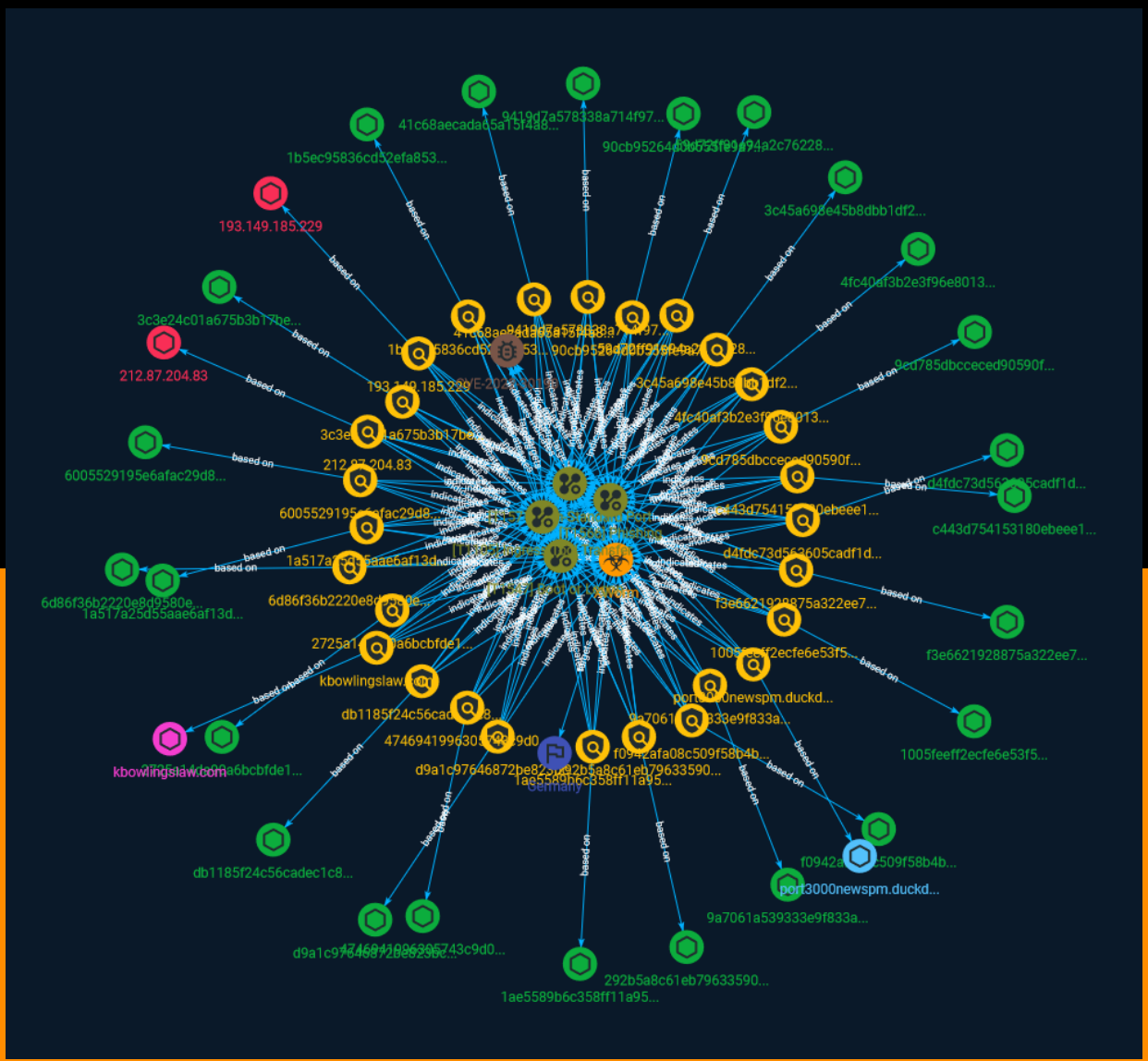

Table of contents

Overview

Entities

Observables

External References

Overview

Description

An in-depth technical analysis of an ongoing XWorm malware attack campaign and how it is being targeted.

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

Non-Standard Port

ID

T1571

Description

Adversaries may communicate using a protocol and port pairing that are typically not associated. For example, HTTPS over port 8088(Citation: Symantec Elfin Mar 2019) or port 587(Citation: Fortinet Agent Tesla April 2018) as opposed to the traditional port 443. Adversaries may make changes to the standard port used by a protocol to bypass filtering or muddle analysis/parsing of network data. Adversaries may also make changes to victim systems to abuse non-standard ports. For example, Registry keys and other configuration settings can be used to modify protocol and port pairings.(Citation: change_rdp_port_conti)

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

Ingress Tool Transfer

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)). 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) 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)

Indicator

Name

9a7061a539333e9f833a589197a60258ebb820bba5f1f29d5b31453e8e392d0f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9a7061a539333e9f833a589197a60258ebb820bba5f1f29d5b31453e8e392d0f']

Name

2725a14da90a6bcbfde174df8b0e95179b617aa14ec07a2d1fc71000310ad913

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2725a14da90a6bcbfde174df8b0e95179b617aa14ec07a2d1fc71000310ad913']

Name

59d72ff91e94a2c762285cce3bcb3e94e8d14608c2eeecacdcd6fe720c3ad5f2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '59d72ff91e94a2c762285cce3bcb3e94e8d14608c2eeecacdcd6fe720c3ad5f2']

Name

292b5a8c61eb79633590b6b13c0b41388ccad3535b55ed822b887d6d15d61be4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '292b5a8c61eb79633590b6b13c0b41388ccad3535b55ed822b887d6d15d61be4']

Name

3c3e24c01a675b3b17bee9c8f560a33c3ecca8c44442fd5b3dd8c0f4429f279b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3c3e24c01a675b3b17bee9c8f560a33c3ecca8c44442fd5b3dd8c0f4429f279b']

Name

9cd785dbcceced90590f87734b8a3dbc066a26bd90d4e4db9a480889731b6d29

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9cd785dbcceced90590f87734b8a3dbc066a26bd90d4e4db9a480889731b6d29']

Name

db1185f24c56cadec1c85a33b0efeb2d803ff00abf4c9df1e00d860683068415

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'db1185f24c56cadec1c85a33b0efeb2d803ff00abf4c9df1e00d860683068415']

Name

41c68aecada65a15f4a8bea52cc25033a1b73ff7340cd3865d55c61ded566e81

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '41c68aecada65a15f4a8bea52cc25033a1b73ff7340cd3865d55c61ded566e81']

Name

port3000newspm.duckdns.org

Pattern Type

stix

Pattern

[hostname:value = 'port3000newspm.duckdns.org']

Name

6005529195e6afac29d8c62091ee7990e92b7a80b391b03c34c8a8fbf019fce6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6005529195e6afac29d8c62091ee7990e92b7a80b391b03c34c8a8fbf019fce6']

Name

4fc40af3b2e3f96e8013a7187e5cb4ce1a00a9528823f789cb8aca09c51143c6

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '4fc40af3b2e3f96e8013a7187e5cb4ce1a00a9528823f789cb8aca09c51143c6']
Name
d9a1c97646872be823bce7e37325f9869daa5593f3ced37024dc5188243639be
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'd9a1c97646872be823bce7e37325f9869daa5593f3ced37024dc5188243639be']
Name
1b5ec95836cd52efa853ba3fa76d0849e4094b32048952a7ac0676d34f251776
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '1b5ec95836cd52efa853ba3fa76d0849e4094b32048952a7ac0676d34f251776']

Name

f3e6621928875a322ee7230ccf186bdaa5609118c4a6d1c2f4026adfb8e88744

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f3e6621928875a322ee7230ccf186bdaa5609118c4a6d1c2f4026adfb8e88744']

Name

6d86f36b2220e8d9580e6708856fa74f37f7aa35db1a708e17ecacf0de3d5d2e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6d86f36b2220e8d9580e6708856fa74f37f7aa35db1a708e17ecacf0de3d5d2e']

Name

90cb95264d0b555fe9a760de404196ac183a958c9cc1aad0689598e35fbb0c3b

Description

ConventionEngine_Anomaly_MultiPDB_Double

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '90cb95264d0b555fe9a760de404196ac183a958c9cc1aad0689598e35fbb0c3b']

Name

f0942afa08c509f58b4b9f02cae4581ebf712f2f1763f1a2ffb8f9d964e335ae

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f0942afa08c509f58b4b9f02cae4581ebf712f2f1763f1a2ffb8f9d964e335ae']

Name

212.87.204.83

Description

ISP: Delis LLC **OS:** Windows (Build 10.0.17763) ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 200 OK Date: Fri, 28 Apr 2023 01:16:14 GMT Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Content-Length: 1570 Content-Type: text/html; charset=UTF-8 ``` ---------- **135:** ``` Microsoft RPC Endpoint Mapper d95afe70-a6d5-4259-822e-2c84da1ddb0d version: v1.0 protocol: [MS-RSP]: Remote Shutdown Protocol provider: wininit.exe ncacn_ip_tcp: 212.87.204.83:49664 ncalrpc: WindowsShutdown ncacn_np: \\WIN-HM6FI4VOIEP\PIPE\InitShutdown ncalrpc: WMsgKRpc04BD70 76f226c3-ec14-4325-8a99-6a46348418af version: v1.0 provider: winlogon.exe ncalrpc: WindowsShutdown ncacn_np: \\WIN-HM6FI4VOIEP\PIPE\InitShutdown ncalrpc: WMsgKRpc04BD70 ncalrpc: WMsgKRpc04C241 ncalrpc: WMsgKRpc0908562 fc48cd89-98d6-4628-9839-86f7a3e4161a version: v1.0 ncalrpc: dabrpc ncalrpc: csebpub

ncalrpc: LRPC-0bc5be8d36157f2b44 ncalrpc: LRPC-6088293f44102f5dc2 ncalrpc: LRPC-6e6302da68b5b4afa8 ncalrpc: LRPC-f457b2a28eef62461c ncalrpc: LRPC-d9c4eaffa54d0566ad ncalrpc: OLE5AEDC7EDE1EA58A7698E7577978E ncalrpc: LRPC-17689c4c9329431e55 ncalrpc: actkernel ncalrpc: umpo d09bdeb5-6171-4a34-bfe2-06fa82652568 version: v1.0 ncalrpc: csebpub ncalrpc: LRPC-0bc5be8d36157f2b44 ncalrpc: LRPC-6088293f44102f5dc2 ncalrpc: LRPC-6e6302da68b5b4afa8 ncalrpc: LRPC-f457b2a28eef62461c ncalrpc: LRPC-d9c4eaffa54d0566ad ncalrpc: OLE5AEDC7EDE1EA58A7698E7577978E ncalrpc: LRPC-17689c4c9329431e55 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-6088293f44102f5dc2 ncalrpc: LRPC-6e6302da68b5b4afa8 ncalrpc: LRPC-f457b2a28eef62461c ncalrpc: LRPC-d9c4eaffa54d0566ad ncalrpc: OLE5AEDC7EDE1EA58A7698E7577978E ncalrpc: LRPC-17689c4c9329431e55 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-6e6302da68b5b4afa8 ncalrpc: LRPC-f457b2a28eef62461c ncalrpc: LRPC-d9c4eaffa54d0566ad ncalrpc: OLE5AEDC7EDE1EA58A7698E7577978E ncalrpc: LRPC-17689c4c9329431e55 ncalrpc: actkernel ncalrpc: umpo ncalrpc: LRPC-82ea6c6a9fbc5b892a ncalrpc: LRPC-ecb8fe97ff7d6aa8b1 697dcda9-3ba9-4eb2-9247-e11f1901b0d2 version: v1.0 ncalrpc: LRPC-0bc5be8d36157f2b44 ncalrpc: LRPC-6088293f44102f5dc2 ncalrpc: LRPC-6e6302da68b5b4afa8 ncalrpc: LRPC-f457b2a28eef62461c ncalrpc: LRPC-d9c4eaffa54d0566ad ncalrpc: OLE5AEDC7EDE1EA58A7698E7577978E ncalrpc: LRPC-17689c4c9329431e55 ncalrpc: actkernel ncalrpc: umpo 9b008953-f195-4bf9-bde0-4471971e58ed version: v1.0 ncalrpc: LRPC-6088293f44102f5dc2 ncalrpc: LRPC-6e6302da68b5b4afa8 ncalrpc: LRPC-f457b2a28eef62461c ncalrpc: LRPC-d9c4eaffa54d0566ad ncalrpc: OLE5AEDC7EDE1EA58A7698E7577978E ncalrpc: LRPC-17689c4c9329431e55 ncalrpc: actkernel ncalrpc: umpo dd59071b-3215-4c59-8481-972edadc0f6a version: v1.0 ncalrpc: umpo 0d47017b-b33b-46ad-9e18-fe96456c5078 version: v1.0 ncalrpc: umpo 95406f0b-b239-4318-91bb-cea3a46ff0dc version: v1.0 ncalrpc: umpo 4ed8abcc-f1e2-438b-981f-bb0e8abc010c version: v1.0 ncalrpc: umpo 0ff1f646-13bb-400a-ab50-9a78f2b7a85a version: v1.0 ncalrpc: umpo 6982a06e-5fe2-46b1-b39c-a2c545bfa069 version: v1.0 ncalrpc: umpo 082a3471-31b6-422a-b931-a54401960c62 version: v1.0 ncalrpc: umpo fae436b0-b864-4a87-9eda-298547cd82f2 version: v1.0 ncalrpc: umpo e53d94ca-7464-4839-b044-09a2fb8b3ae5 version: v1.0 ncalrpc: umpo 178d84be-9291-4994-82c6-3f909aca5a03 version: v1.0 ncalrpc: umpo 4dace966-a243-4450-ae3f-9b7bcb5315b8 version: v2.0 ncalrpc: umpo 1832bcf6-cab8-41d4-85d2-c9410764f75a version: v1.0 ncalrpc: umpo c521facf-09a9-42c5-b155-72388595cbf0 version: v0.0 ncalrpc: umpo 2c7fd9ce-e706-4b40-b412-953107ef9bb0 version: v0.0 ncalrpc: umpo 88abcbc3-34ea-76ae-8215-767520655a23 version: v0.0 ncalrpc: LRPC-f457b2a28eef62461c ncalrpc: LRPC-d9c4eaffa54d0566ad ncalrpc: OLE5AEDC7EDE1EA58A7698E7577978E ncalrpc: LRPC-17689c4c9329431e55 ncalrpc: actkernel ncalrpc: umpo 76c217bc-c8b4-4201-a745-373ad9032b1a version: v1.0 ncalrpc: LRPC-f457b2a28eef62461c ncalrpc: LRPC-d9c4eaffa54d0566ad ncalrpc: OLE5AEDC7EDE1EA58A7698E7577978E ncalrpc: LRPC-17689c4c9329431e55 ncalrpc: actkernel ncalrpc: umpo 55e6b932-1979-45d6-90c5-7f6270724112 version: v1.0 ncalrpc: LRPC-f457b2a28eef62461c ncalrpc: LRPC-d9c4eaffa54d0566ad ncalrpc: OLE5AEDC7EDE1EA58A7698E7577978E ncalrpc: LRPC-17689c4c9329431e55 ncalrpc: actkernel ncalrpc: umpo 857fb1be-084f-4fb5-b59c-4b2c4be5f0cf version: v1.0 ncalrpc: LRPC-

d9c4eaffa54d0566ad ncalrpc: OLE5AEDC7EDE1EA58A7698E7577978E ncalrpc: LRPC-17689c4c9329431e55 ncalrpc: actkernel ncalrpc: umpo b8cadbaf-e84b-46b9-84f2-6f71c03f9e55 version: v1.0 ncalrpc: LRPC-d9c4eaffa54d0566ad ncalrpc: OLE5AEDC7EDE1EA58A7698E7577978E ncalrpc: LRPC-17689c4c9329431e55 ncalrpc: actkernel ncalrpc: umpo 20c40295-8dba-48e6-aebf-3e78ef3bb144 version: v1.0 ncalrpc: LRPC-d9c4eaffa54d0566ad ncalrpc: OLE5AEDC7EDE1EA58A7698E7577978E ncalrpc: LRPC-17689c4c9329431e55 ncalrpc: actkernel ncalrpc: umpo 2513bcbe-6cd4-4348-855e-7efb3c336dd3 version: v1.0 ncalrpc: LRPC-d9c4eaffa54d0566ad ncalrpc: OLE5AEDC7EDE1EA58A7698E7577978E ncalrpc: LRPC-17689c4c9329431e55 ncalrpc: actkernel ncalrpc: umpo 0d3e2735-cea0-4ecc-a9e2-41a2d81aed4e version: v1.0 ncalrpc: LRPC-17689c4c9329431e55 ncalrpc: actkernel ncalrpc: umpo c605f9fb-f0a3-4e2a-a073-73560f8d9e3e version: v1.0 ncalrpc: LRPC-17689c4c9329431e55 ncalrpc: actkernel ncalrpc: umpo 1b37ca91-76b1-4f5e-a3c7-2abfc61f2bb0 version: v1.0 ncalrpc: LRPC-17689c4c9329431e55 ncalrpc: actkernel ncalrpc: umpo 8bfc3be1-6def-4e2d-af74-7c47cd0ade4a version: v1.0 ncalrpc: LRPC-17689c4c9329431e55 ncalrpc: actkernel ncalrpc: umpo 2d98a740-581d-41b9-aa0d-a88b9d5ce938 version: v1.0 ncalrpc: LRPC-17689c4c9329431e55 ncalrpc: actkernel ncalrpc: umpo 0361ae94-0316-4c6c-8ad8-c594375800e2 version: v1.0 ncalrpc: umpo 5824833b-3c1a-4ad2-bdfd-c31d19e23ed2 version: v1.0 ncalrpc: umpo bdaa0970-413b-4a3e-9e5d-f6dc9d7e0760 version: v1.0 ncalrpc: umpo 3b338d89-6cfa-44b8-847e-531531bc9992 version: v1.0 ncalrpc: umpo 8782d3b9-ebbd-4644-a3d8-e8725381919b version: v1.0 ncalrpc: umpo 085b0334-e454-4d91-9b8c-4134f9e793f3 version: v1.0 ncalrpc: umpo 4bec6bb8-b5c2-4b6f-b2c1-5da5cf92d0d9 version: v1.0 ncalrpc: umpo 51a227ae-825b-41f2-b4a9-1ac9557a1018 version: v1.0 annotation: Ngc Pop Key Service ncacn_ip_tcp: 212.87.204.83:49665 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\WIN-HM6FI4VOIEP\pipe\lsass 8fb74744-b2ff-4c00-be0d-9ef9a191fe1b version: v1.0 annotation: Ngc Pop Key Service ncacn_ip_tcp: 212.87.204.83:49665 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\WIN-HM6FI4VOIEP\pipe\lsass b25a52bf-e5dd-4f4a-aea6-8ca7272a0e86 version: v2.0 annotation: KeyIso ncacn_ip_tcp: 212.87.204.83:49665 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\WIN-HM6FI4VOIEP\pipe\lsass 12345778-1234-abcd-ef00-0123456789ac version: v1.0 protocol: [MS-SAMR]: Security Account Manager (SAM) Remote Protocol provider: samsrv.dll ncacn_ip_tcp: 212.87.204.83:49665 ncalrpc: samss lpc ncalrpc: SidKey Local End Point ncalrpc: protected_storage ncalrpc: lsasspirpc ncalrpc: lsapolicylookup ncalrpc: LSA_EAS_ENDPOINT ncalrpc: LSA_IDPEXT_ENDPOINT ncalrpc: lsacap ncalrpc: LSARPC_ENDPOINT ncalrpc: securityevent ncalrpc: audit ncacn_np: \\WIN-HM6FI4VOIEP\pipe\lsass c9ac6db5-82b7-4e55-ae8a-e464ed7b4277 version: v1.0 annotation:

Impl friendly name provider: sysntfy.dll ncalrpc: LRPC-5c7269018c57b0db7e ncalrpc: IUserProfile2 ncalrpc: LRPC-ecadb26fa3882f6282 ncalrpc: LRPC-3872857f2764028c4a ncalrpc: senssvc ncalrpc: LRPC-e69ff4d55813dc2786 f3f09ffd-fbcf-4291-944d-70ad6e0e73bb version: v1.0 ncalrpc: LRPC-9ceffface70a4becdc3 ncalrpc: LRPC-03adfe44175c6db142 30adc50c-5cbc-46ce-9a0e-91914789e23c version: v1.0 annotation: NRP server endpoint provider: nrpsrv.dll ncalrpc: LRPC-b714de095ad2d82448 a500d4c6-0dd1-4543-bc0c-d5f93486eaf8 version: v1.0 ncalrpc: LRPC-63e9a80b8a109b16dd ncalrpc: LRPC-82ea6c6a9fbc5b892a e40f7b57-7a25-4cd3-a135-7f7d3df9d16b version: v1.0 annotation: Network Connection Broker server endpoint ncalrpc: LRPC-1656638adba9f4aecf ncalrpc: OLEE7BC7529985346EDE8B6EA2762E8 ncalrpc: LRPC-5a9e7ee94319c890db ncalrpc: LRPC-ecb8fe97ff7d6aa8b1 880fd55e-43b9-11e0-b1a8-cf4edfd72085 version: v1.0 annotation: KAPI Service endpoint ncalrpc: LRPC-1656638adba9f4aecf ncalrpc: OLEE7BC7529985346EDE8B6EA2762E8 ncalrpc: LRPC-5a9e7ee94319c890db ncalrpc: LRPC-ecb8fe97ff7d6aa8b1 5222821f-d5e2-4885-84f1-5f6185a0ec41 version: v1.0 annotation: Network Connection Broker server endpoint for NCB Reset module ncalrpc: LRPC-5a9e7ee94319c890db ncalrpc: LRPC-ecb8fe97ff7d6aa8b1 7ea70bcf-48af-4f6a-8968-6a440754d5fa version: v1.0 annotation: NSI server endpoint provider: nsisvc.dll ncalrpc: LRPC-9bd07098464e28f358 2eb08e3e-639f-4fba-97b1-14f878961076 version: v1.0 annotation: Group Policy RPC Interface provider: gpsvc.dll ncalrpc: LRPC-809ed632a847414f53 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d6 version: v1.0 annotation: DHCPv6 Client LRPC Endpoint provider: dhcpcsvc6.dll ncalrpc: dhcpcsvc6 ncalrpc: dhcpcsvc 3c4728c5-f0ab-448b-bda1-6ce01eb0a6d5 version: v1.0 annotation: DHCP Client LRPC Endpoint provider: dhcpcsvc.dll ncalrpc: dhcpcsvc df4df73a-c52d-4e3a-8003-8437fdf8302a version: v0.0 annotation: WM_WindowManagerRPC\Server ncalrpc: LRPC-9e0c3c7afffc18d187 f6beaff7-1e19-4fbb-9f8f-b89e2018337c version: v1.0 annotation: Event log TCPIP protocol: [MS-EVEN6]: EventLog Remoting Protocol provider: wevtsvc.dll ncacn_ip_tcp: 212.87.204.83:49666 ncacn_np: \\WIN-HM6FI4VOIEP\pipe\eventlog ncalrpc: eventlog 3a9ef155-691d-4449-8d05-09ad57031823 version: v1.0 ncacn_ip_tcp: 212.87.204.83:49667 ncalrpc: LRPC-892418c80dfd2a3343 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-HM6FI4VOIEP\PIPE\atsvc ncalrpc: LRPC-02fbd59979171061d8 86d35949-83c9-4044-b424-db363231fd0c version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: schedsvc.dll ncacn_ip_tcp: 212.87.204.83:49667 ncalrpc: LRPC-892418c80dfd2a3343 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-HM6FI4VOIEP\PIPE\atsvc ncalrpc: LRPC-02fbd59979171061d8 33d84484-3626-47ee-8c6f-e7e98b113be1 version: v2.0 ncalrpc: LRPC-892418c80dfd2a3343 ncalrpc: ubpmtaskhostchannel ncacn_np: \\WIN-HM6FI4VOIEP\PIPE\atsvc ncalrpc: LRPC-02fbd59979171061d8 378e52b0-c0a9-11cf-822d-00aa0051e40f version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\WIN-HM6FI4VOIEP\PIPE\atsvc ncalrpc: LRPC-02fbd59979171061d8 1ff70682-0a51-30e8-076d-740be8cee98b version: v1.0 protocol: [MS-TSCH]: Task Scheduler Service Remoting Protocol provider: taskcomp.dll ncacn_np: \\WIN-HM6FI4VOIEP\PIPE\atsvc ncalrpc: LRPC-02fbd59979171061d8 0a74ef1c-41a4-4e06-83ae-dc74fb1cdd53 version: v1.0 provider: schedsvc.dll ncalrpc: LRPC-02fbd59979171061d8 3473dd4d-2e88-4006-9cba-22570909dd10 version: v5.256

annotation: WinHttp Auto-Proxy Service ncalrpc: 9f6111f6-a5e6-47e7-89ba-ad007106736a ncalrpc: LRPC-d7d28a8bce570ee912 2fb92682-6599-42dc-ae13-bd2ca89bd11c version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-1a967301d5773385fe ncalrpc: LRPC-3651ac885c86a4e0dc ncalrpc: LRPC-5c196d32b7d7a15b7f ncalrpc: LRPC-026e9188b02e0271e6 f47433c3-3e9d-4157-aad4-83aa1f5c2d4c version: v1.0 annotation: Fw APIs ncalrpc: LRPC-3651ac885c86a4e0dc ncalrpc: LRPC-5c196d32b7d7a15b7f ncalrpc: LRPC-026e9188b02e0271e6 7f9d11bf-7fb9-436b-a812-b2d50c5d4c03 version: v1.0 annotation: Fw APIs provider: MPSSVC.dll ncalrpc: LRPC-5c196d32b7d7a15b7f ncalrpc: LRPC-026e9188b02e0271e6 dd490425-5325-4565-b774-7e27d6c09c24 version: v1.0 annotation: Base Firewall Engine API provider: BFE.DLL ncalrpc: LRPC-026e9188b02e0271e6 7f1343fe-50a9-4927-a778-0c5859517bac version: v1.0 annotation: DfsDs service ncacn_np: \\WIN-HM6FI4VOIEP\PIPE\wkssvc ncalrpc: LRPC-1c4f9a8ab4e127804a eb081a0d-10ee-478a-a1dd-50995283e7a8 version: v3.0 annotation: Witness Client Test Interface ncalrpc: LRPC-1c4f9a8ab4e127804a f2c9b409-c1c9-4100-8639-d8ab1486694a version: v1.0 annotation: Witness Client Upcall Server ncalrpc: LRPC-1c4f9a8ab4e127804a c2d1b5dd-fa81-4460-9dd6-e7658b85454b version: v1.0 ncalrpc: LRPC-6908a0500cdc19bae1 f44e62af-dab1-44c2-8013-049a9de417d6 version: v1.0 ncalrpc: LRPC-6908a0500cdc19bae1 7aeb6705-3ae6-471a-882d-f39c109edc12 version: v1.0 ncalrpc: LRPC-6908a0500cdc19bae1 e7f76134-9ef5-4949-a2d6-3368cc0988f3 version: v1.0 ncalrpc: LRPC-6908a0500cdc19bae1 b37f900a-eae4-4304-a2ab-12bb668c0188 version: v1.0 ncalrpc: LRPC-6908a0500cdc19bae1 abfb6ca3-0c5e-4734-9285-0aee72fe8d1c version: v1.0 ncalrpc: LRPC-6908a0500cdc19bae1 a398e520-d59a-4bdd-aa7a-3c1e0303a511 version: v1.0 annotation: IKE/Authip API provider: IKEEXT.DLL ncalrpc: LRPC-6f5ad20afe7a4ccf08 30b044a5-a225-43f0-b3a4-e060df91f9c1 version: v1.0 provider: certprop.dll ncalrpc: LRPC-1c3011e36c663a69b4 b58aa02e-2884-4e97-8176-4ee06d794184 version: v1.0 provider: sysmain.dll ncalrpc: LRPC-1c6269ff89e60c86a8 76f03f96-cdfd-44fc-a22c-64950a001209 version: v1.0 protocol: [MS-PAR]: Print System Asynchronous Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 212.87.204.83:49668 ncalrpc: LRPC-0ce4d196836e317993 4a452661-8290-4b36-8fbe-7f4093a94978 version: v1.0 provider: spoolsv.exe ncacn_ip_tcp: 212.87.204.83:49668 ncalrpc: LRPC-0ce4d196836e317993 ae33069b-a2a8-46ee-a235-ddfd339be281 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 212.87.204.83:49668 ncalrpc: LRPC-0ce4d196836e317993 0b6edbfa-4a24-4fc6-8a23-942b1eca65d1 version: v1.0 protocol: [MS-PAN]: Print System Asynchronous Notification Protocol provider: spoolsv.exe ncacn_ip_tcp: 212.87.204.83:49668 ncalrpc: LRPC-0ce4d196836e317993 12345678-1234-abcd-ef00-0123456789ab version: v1.0 protocol: [MS-RPRN]: Print System Remote Protocol provider: spoolsv.exe ncacn_ip_tcp: 212.87.204.83:49668 ncalrpc: LRPC-0ce4d196836e317993 29770a8f-829b-4158-90a2-78cd488501f7 version: v1.0 ncacn_ip_tcp: 212.87.204.83:49669 ncacn_np: \\WIN-HM6FI4VOIEP\pipe\SessEnvPublicRpc ncalrpc: SessEnvPrivateRpc ncalrpc: LRPC-e69ff4d55813dc2786 c49a5a70-8a7f-4e70-ba16-1e8f1f193ef1 version: v1.0 annotation: Adh APIs ncalrpc: OLE1DF992CF7A44F032A517EF0789BA ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-787c7d668cdc88d2cd c36be077-e14b-4fe9-8abc-e856ef4f048b version: v1.0 annotation: Proxy Manager client server endpoint ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-787c7d668cdc88d2cd 2e6035b2-

e8f1-41a7-a044-656b439c4c34 version: v1.0 annotation: Proxy Manager provider server endpoint ncalrpc: TeredoControl ncalrpc: TeredoDiagnostics ncalrpc: LRPC-787c7d668cdc88d2cd 552d076a-cb29-4e44-8b6a-d15e59e2c0af version: v1.0 annotation: IP Transition Configuration endpoint provider: iphlpsvc.dll ncalrpc: LRPC-787c7d668cdc88d2cd 0d3c7f20-1c8d-4654-a1b3-51563b298bda version: v1.0 annotation: UserMgrCli ncalrpc: LRPC-0de79723f782600d1f ncalrpc: OLE84CD5680EBE05DBE1AF3B9F69E07 b18fbab6-56f8-4702-84e0-41053293a869 version: v1.0 annotation: UserMgrCli ncalrpc: LRPC-0de79723f782600d1f ncalrpc: OLE84CD5680EBE05DBE1AF3B9F69E07 1a0d010f-1c33-432c-b0f5-8cf4e8053099 version: v1.0 annotation: IdSegSrv service ncalrpc: LRPC-953dc181c116839d9e 98716d03-89ac-44c7-bb8c-285824e51c4a version: v1.0 annotation: XactSrv service provider: srvsvc.dll ncalrpc: LRPC-953dc181c116839d9e 367abb81-9844-35f1-ad32-98f038001003 version: v2.0 protocol: [MS-SCMR]: Service Control Manager Remote Protocol provider: services.exe ncacn_ip_tcp: 212.87.204.83:49670 6b5bdd1e-528c-422c-af8c-a4079be4fe48 version: v1.0 annotation: Remote Fw APIs protocol: [MS-FASP]: Firewall and Advanced Security Protocol provider: FwRemoteSvr.dll ncacn_ip_tcp: 212.87.204.83:49671 ncalrpc: ipsec 98cd761e-e77d-41c8-a3c0-0fb756d90ec2 version: v1.0 ncalrpc: LRPC-4b7104cdcc6688428a d22895ef-aff4-42c5-a5b2-b14466d34ab4 version: v1.0 ncalrpc: LRPC-4b7104cdcc6688428a e38f5360-8572-473e-b696-1b46873beeab version: v1.0 ncalrpc: LRPC-4b7104cdcc6688428a 95095ec8-32ea-4eb0-a3e2-041f97b36168 version: v1.0 ncalrpc: LRPC-4b7104cdcc6688428a fd8be72b-a9cd-4b2c-a9ca-4ded242fbe4d version: v1.0 ncalrpc: LRPC-4b7104cdcc6688428a 4c9dbf19-d39e-4bb9-90ee-8f7179b20283 version: v1.0 ncalrpc: LRPC-4b7104cdcc6688428a 906b0ce0-c70b-1067-b317-00dd010662da version: v1.0 protocol: [MS-CMPO]: MSDTC Connection Manager: provider: msdtcprx.dll ncalrpc: LRPC-6168041faf03239783 ncalrpc: LRPC-6168041faf03239783 ncalrpc: LRPC-6168041faf03239783 12e65dd8-887f-41ef-91bf-8d816c42c2e7 version: v1.0 annotation: Secure Desktop LRPC interface provider: winlogon.exe ncalrpc: WMsgKRpc0908562 b1ef227e-dfa5-421e-82bb-67a6a129c496 version: v0.0 ncalrpc: LRPC-026ec5e40ea082dce4 ncalrpc: OLEC27343A2BBD700D3888C4B990D01 0fc77b1a-95d8-4a2e-a0c0-cff54237462b version: v0.0 ncalrpc: LRPC-026ec5e40ea082dce4 ncalrpc: OLEC27343A2BBD700D3888C4B990D01 8ec21e98-b5ce-4916-a3d6-449fa428a007 version: v0.0 ncalrpc: LRPC-026ec5e40ea082dce4 ncalrpc: OLEC27343A2BBD700D3888C4B990D01 0767a036-0d22-48aa-ba69-b619480f38cb version: v1.0 annotation: PcaSvc provider: pcasvc.dll ncalrpc: LRPC-9096a5f7bf37d324d9 54b4c689-969a-476f-8dc2-990885e9f562 version: v0.0 ncalrpc: LRPC-739c5652c246cf8323 be7f785e-0e3a-4ab7-91de-7e46e443be29 version: v0.0 ncalrpc: LRPC-739c5652c246cf8323 bf4dc912-e52f-4904-8ebe-9317c1bdd497 version: v1.0 ncalrpc: LRPC-bacd438051eb248396 ncalrpc: OLE8BD45F117C92BDB7F63D46B542CE 58e604e8-9adb-4d2e-a464-3b0683fb1480 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-a7df6e2b25f4824a63 fd7a0523-dc70-43dd-9b2e-9c5ed48225b1 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-a7df6e2b25f4824a63 5f54ce7d-5b79-4175-8584-cb65313a0e98 version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-a7df6e2b25f4824a63 201ef99a-7fa0-444c-9399-19ba84f12a1a version: v1.0 annotation: AppInfo provider: appinfo.dll ncalrpc: LRPC-a7df6e2b25f4824a63 0497b57d-2e66-424f-a0c6-157cd5d41700 version: v1.0 annotation: AppInfo ncalrpc: LRPC-a7df6e2b25f4824a63

a4b8d482-80ce-40d6-934d-b22a01a44fe7 version: v1.0 annotation: LicenseManager ncalrpc: LicenseServiceEndpoint ``` ---------- **139:** ``` \x83\x00\x00\x01\x8f ``` ---------- **443:** ``` HTTP/1.1 200 OK Date: Wed, 26 Apr 2023 00:12:24 GMT Server: Apache/2.4.56 (Win64) OpenSSL/1.1.1t PHP/8.2.4 Last-Modified: Mon, 16 Jan 2023 14:24:24 GMT ETag: "3c3e-5f2625701b600" Accept-Ranges: bytes Content-Length: 15422 Content-Type: text/html ``` HEARTBLEED: 2023/04/26 00:12:29 212.87.204.83:443 - SAFE ---------- **3306:** ``` MariaDB: Error Message: Host '224.99.220.75' is not allowed to connect to this MariaDB server Error Code: 1130 ``` ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 10/Windows Server 2019 OS Build: 10.0.17763 Target Name: WIN-HM6FI4VOIEP NetBIOS Domain Name: WIN-HM6FI4VOIEP NetBIOS Computer Name: WIN-HM6FI4VOIEP DNS Domain Name: WIN-HM6FI4VOIEP FQDN: WIN-HM6FI4VOIEP ; Administrator SES ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '212.87.204.83']

Name

c443d754153180ebeee1106d5eecf1024e063413f3f92a29c6c95a08c6f2e633

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c443d754153180ebeee1106d5eecf1024e063413f3f92a29c6c95a08c6f2e633']

Name

4746941996305743c9d0bcb96ed4b2b930355cd8782098aa5600b42131314308

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4746941996305743c9d0bcb96ed4b2b930355cd8782098aa5600b42131314308']

Name

9419d7a578338a714f976fb2b9eb320049422ec7059cedcc4a8baf144c4df41b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9419d7a578338a714f976fb2b9eb320049422ec7059cedcc4a8baf144c4df41b']

Name

1005feeff2ecfe6e53f53f63a2364de8418863d83e256322ca82e939dae95e45

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1005feeff2ecfe6e53f53f63a2364de8418863d83e256322ca82e939dae95e45']

Name

1a517a25d55aae6af13d025b1d1edee7fb185b90155f30e195f58cbf4c6b36fe

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1a517a25d55aae6af13d025b1d1edee7fb185b90155f30e195f58cbf4c6b36fe']

Name

3c45a698e45b8dbb1df206dec08c8792087619e54c0c9fc0f064bd9a47a84f16

Description

ALF:Trojan:MSIL/AgentTesla.KM

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3c45a698e45b8dbb1df206dec08c8792087619e54c0c9fc0f064bd9a47a84f16']

Name

1ae5589b6c358ff11a9555a7265ba5f0709be7a865e2cf51af04eb17b2a2ce18

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1ae5589b6c358ff11a9555a7265ba5f0709be7a865e2cf51af04eb17b2a2ce18']

Name

193.149.185.229

Description

ISP: BL Networks **OS:** Debian ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDssr9co/hqLhnC2iHijE1SG0iBKP7d0iAj8e4GteU3kznoFbRQyCTUJTtA3Bnf2HSemf3HV/2V8EAG2MXvnyu2XpsMaRK58aJBHD8y+QaZPMxi3pDET8PAvMM9 /7pUNdBQyCDBo088E/eJeuV+4ORoa864kwVtFzEmbiWtt18Mpcg8RE4AARDo+VG3NlTBMCR+sjvF aX5/AqQQnIvVz2seD1D4PUXnBjkG3yYeljZnI8NWFxit43daskX4tJWQvF6yKYHHJv76A97R4LAz7lpT6gAvr+1919fFaJ7Z79e4xWhncknPSUDDaP6VioWKLZqbO9CLv2w8vf19gkXwy4gR0nGVAVlQIrpTkcq3X2rhVoYPDj4w6kal90uz1gGnDU+9ZWDDPkFEcErLxb4vJT4ltBjXAM703jOn6hLbckd3KQfNclfVLMXUhNMJTHCLxUeZ/KNY4bQD+N5LDkDSwq5R4fWgYTz0PBfZnnP6k5xqbxyEBwF1TQXm iPKhJ7G5BNs= Fingerprint: df:a1:4a:e8:b7:f5:a2:aa:63:e1:d2:22:b4:f2:aa:5a 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 = '193.149.185.229']

Name

d4fdc73d563605cadf1ded9b644f21e8dae0f65870890357e5bc554bbc66bf74

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd4fdc73d563605cadf1ded9b644f21e8dae0f65870890357e5bc554bbc66bf74']

Name

kbowlingslaw.com

Pattern Type

stix

Pattern

[domain-name:value = 'kbowlingslaw.com']

Country

Name
Germany

Malware

Name
XWorm

Domain-Name

Value
kbowlingslaw.com

StixFile

Value
2725a14da90a6bcbfde174df8b0e95179b617aa14ec07a2d1fc71000310ad913
d9a1c97646872be823bce7e37325f9869daa5593f3ced37024dc5188243639be
6005529195e6afac29d8c62091ee7990e92b7a80b391b03c34c8a8fbf019fce6
1005feeff2ecfe6e53f53f63a2364de8418863d83e256322ca82e939dae95e45
1ae5589b6c358ff11a9555a7265ba5f0709be7a865e2cf51af04eb17b2a2ce18
db1185f24c56cadec1c85a33b0efeb2d803ff00abf4c9df1e00d860683068415
41c68aecada65a15f4a8bea52cc25033a1b73ff7340cd3865d55c61ded566e81
3c45a698e45b8dbb1df206dec08c8792087619e54c0c9fc0f064bd9a47a84f16
9cd785dbcceced90590f87734b8a3dbc066a26bd90d4e4db9a480889731b6d29
1a517a25d55aae6af13d025b1d1edee7fb185b90155f30e195f58cbf4c6b36fe
6d86f36b2220e8d9580e6708856fa74f37f7aa35db1a708e17ecacf0de3d5d2e
4746941996305743c9d0bcb96ed4b2b930355cd8782098aa5600b42131314308
59d72ff91e94a2c762285cce3bcb3e94e8d14608c2eeecacdcd6fe720c3ad5f2

9419d7a578338a714f976fb2b9eb320049422ec7059cedcc4a8baf144c4df41b

90cb95264d0b555fe9a760de404196ac183a958c9cc1aad0689598e35fbb0c3b

f3e6621928875a322ee7230ccf186bdaa5609118c4a6d1c2f4026adfb8e88744

4fc40af3b2e3f96e8013a7187e5cb4ce1a00a9528823f789cb8aca09c51143c6

c443d754153180ebeee1106d5eecf1024e063413f3f92a29c6c95a08c6f2e633

d4fdc73d563605cadf1ded9b644f21e8dae0f65870890357e5bc554bbc66bf74

f0942afa08c509f58b4b9f02cae4581ebf712f2f1763f1a2ffb8f9d964e335ae

3c3e24c01a675b3b17bee9c8f560a33c3ecca8c44442fd5b3dd8c0f4429f279b

1b5ec95836cd52efa853ba3fa76d0849e4094b32048952a7ac0676d34f251776

9a7061a539333e9f833a589197a60258ebb820bba5f1f29d5b31453e8e392d0f

292b5a8c61eb79633590b6b13c0b41388ccad3535b55ed822b887d6d15d61be4

Hostname

Value
port3000newspm.duckdns.org

IPv4-Addr

Value
193.149.185.229
212.87.204.83

External References

- https://otx.alienvault.com/pulse/64624bf528c55e0976f2bf71
- https://www.securonix.com/blog/securonix-threat-labs-security-meme4chan-advisory/