

NETMANAGEIT

Intelligence Report

AcidPour | New Embedded Wiper Variant of AcidRain Appears in Ukraine

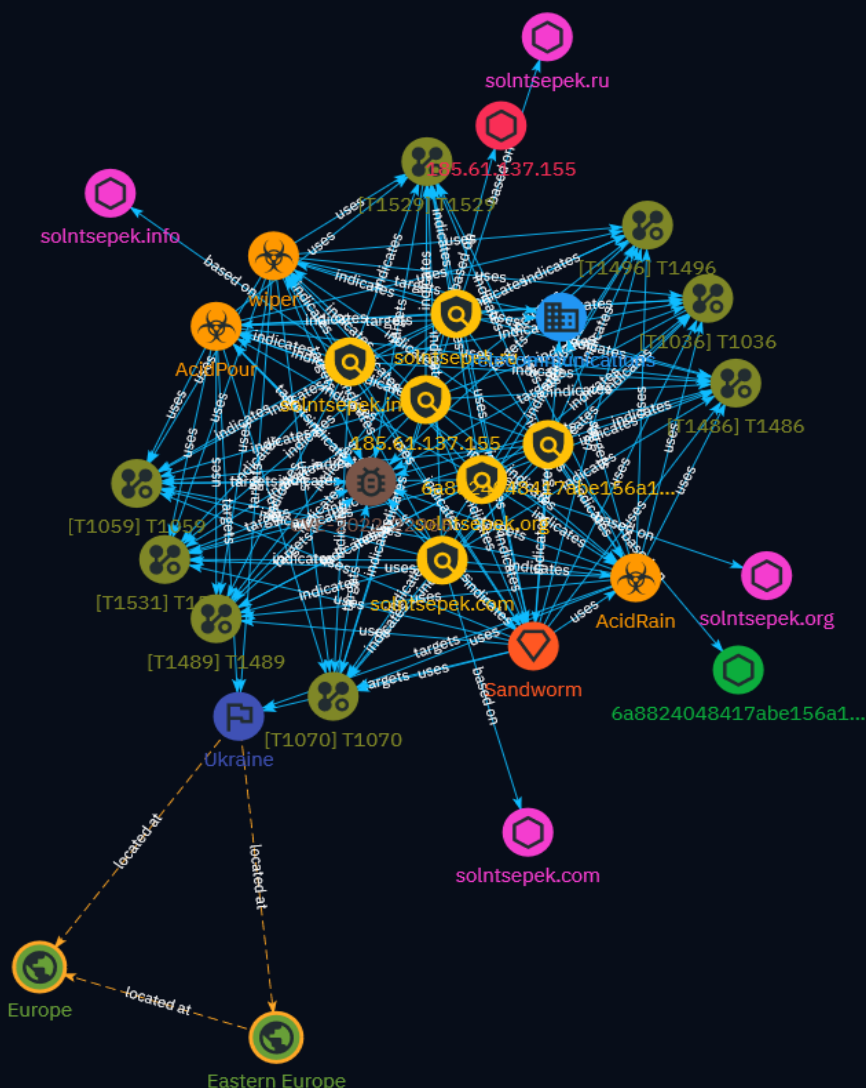


Table of contents

Overview

● Description	4
● Confidence	4
● Content	5

Entities

● Indicator	6
● Malware	9
● Vulnerability	10
● Intrusion-Set	11
● Attack-Pattern	12
● Country	18
● Region	19
● Sector	20

Observables

● Domain-Name	21
● IPv4-Addr	22
● StixFile	23

External References

● External References	24
-----------------------	----

Overview

Description

SentinelLabs discovered a new Linux wiper named AcidPour, a variant of AcidRain used in attacks against Ukraine. AcidPour expands on AcidRain's capabilities to better target Linux devices like networking gear, IoT, RAIDs, and possibly ICS. Its discovery coincides with telecoms disruptions in Ukraine claimed by a GRU hacktivist persona. Technical analysis confirms similarities between AcidPour and AcidRain, linking it to clusters attributed to Russian intelligence.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

solntsepek.ru

Pattern Type

stix

Pattern

[domain-name:value = 'solntsepek.ru']

Name

solntsepek.org

Pattern Type

stix

Pattern

[domain-name:value = 'solntsepek.org']

Name

solntsepek.info

Pattern Type

stix

Pattern

[domain-name:value = 'solntsepek.info']

Name

solntsepek.com

Pattern Type

stix

Pattern

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

Name

185.61.137.155

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.61.137.155']

Name

6a8824048417abe156a16455b8e29170f8347312894fde2aabe644c4995d7728

Pattern Type

stix

Pattern

[file:hashes:'SHA-256' =
'6a8824048417abe156a16455b8e29170f8347312894fde2aabe644c4995d7728']

Malware

Name

AcidPour

Name

AcidRain

Name

wiper

Description

[Wiper](<https://attack.mitre.org/software/S0041>) is a family of destructive malware used in March 2013 during breaches of South Korean banks and media companies. (Citation: Dell Wiper)

Vulnerability

Name

CVE-2022-22965

Description

Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding.

Intrusion-Set

Name
Sandworm

Attack-Pattern

Name

T1529

ID

T1529

Description

Adversaries may shutdown/reboot systems to interrupt access to, or aid in the destruction of, those systems. Operating systems may contain commands to initiate a shutdown/reboot of a machine or network device. In some cases, these commands may also be used to initiate a shutdown/reboot of a remote computer or network device via [Network Device CLI](<https://attack.mitre.org/techniques/T1059/008>) (e.g. `reload`).(Citation: Microsoft Shutdown Oct 2017)(Citation: alert_TA18_106A) Shutting down or rebooting systems may disrupt access to computer resources for legitimate users while also impeding incident response/recovery. Adversaries may attempt to shutdown/reboot a system after impacting it in other ways, such as [Disk Structure Wipe](<https://attack.mitre.org/techniques/T1561/002>) or [Inhibit System Recovery](<https://attack.mitre.org/techniques/T1490>), to hasten the intended effects on system availability.(Citation: Talos Nyetya June 2017) (Citation: Talos Olympic Destroyer 2018)

Name

T1486

ID

T1486

Description

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018) In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](<https://attack.mitre.org/techniques/T1222>) or [System Shutdown/Reboot](<https://attack.mitre.org/techniques/T1529>), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](<https://attack.mitre.org/techniques/T1078>), [OS Credential Dumping](<https://attack.mitre.org/techniques/T1003>), and [SMB/Windows Admin Shares](<https://attack.mitre.org/techniques/T1021/002>).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal Defacement](<https://attack.mitre.org/techniques/T1491/001>), such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020) In cloud environments, storage objects within compromised accounts may also be encrypted.(Citation: Rhino S3 Ransomware Part 1)

Name

T1531

ID

T1531

Description

Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users. Accounts may be deleted, locked, or manipulated (ex: changed credentials) to remove access to accounts. Adversaries may also subsequently log off and/or perform a [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529) to set malicious changes into place.(Citation: CarbonBlack LockerGoga 2019)(Citation: Unit42 LockerGoga 2019) In Windows, [Net](https://attack.mitre.org/software/S0039) utility, `Set-LocalUser` and `Set-ADAccountPassword` [PowerShell](https://attack.mitre.org/techniques/T1059/001) cmdlets may be used by adversaries to modify user accounts. In Linux, the `passwd` utility may be used to change passwords. Accounts could also be disabled by Group Policy. Adversaries who use ransomware or similar attacks may first perform this and other Impact behaviors, such as [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Defacement](https://attack.mitre.org/techniques/T1491), in order to impede incident response/recovery before completing the [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486) objective.

Name

T1496

ID

T1496

Description

Adversaries may leverage the resources of co-opted systems to complete resource-intensive tasks, which may impact system and/or hosted service availability. One common purpose for Resource Hijacking is to validate transactions of cryptocurrency networks and earn virtual currency. Adversaries may consume enough system resources to negatively impact and/or cause affected machines to become unresponsive.(Citation: Kaspersky Lazarus Under The Hood Blog 2017) Servers and cloud-based systems are common targets because of the high potential for available resources, but user endpoint systems may also be compromised and used for Resource Hijacking and cryptocurrency mining.(Citation: CloudSploit - Unused AWS Regions) Containerized environments may also be targeted due to the ease of deployment via exposed APIs and the potential for scaling mining activities by deploying or compromising multiple containers within an environment or cluster. (Citation: Unit 42 Hildegard Malware)(Citation: Trend Micro Exposed Docker APIs)

Additionally, some cryptocurrency mining malware identify then kill off processes for competing malware to ensure it's not competing for resources.(Citation: Trend Micro War of Crypto Miners) Adversaries may also use malware that leverages a system's network bandwidth as part of a botnet in order to facilitate [Network Denial of Service](<https://attack.mitre.org/techniques/T1498>) campaigns and/or to seed malicious torrents.(Citation: GoBotKR) Alternatively, they may engage in proxyjacking by selling use of the victims' network bandwidth and IP address to proxyware services.(Citation: Sysdig Proxyjacking)

Name

T1070

ID

T1070

Description

Adversaries may delete or modify artifacts generated within systems to remove evidence of their presence or hinder defenses. Various artifacts may be created by an adversary or something that can be attributed to an adversary's actions. Typically these artifacts are used as defensive indicators related to monitored events, such as strings from downloaded files, logs that are generated from user actions, and other data analyzed by defenders. Location, format, and type of artifact (such as command or login history) are often specific to each platform. Removal of these indicators may interfere with event collection, reporting, or other processes used to detect intrusion activity. This may compromise the integrity of security solutions by causing notable events to go unreported. This activity may also impede forensic analysis and incident response, due to lack of sufficient data to determine what occurred.

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

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 abusible 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

T1489

ID

T1489

Description

Adversaries may stop or disable services on a system to render those services unavailable to legitimate users. Stopping critical services or processes can inhibit or stop response to an incident or aid in the adversary's overall objectives to cause damage to the environment.(Citation: Talos Olympic Destroyer 2018)(Citation: Novetta Blockbuster)
Adversaries may accomplish this by disabling individual services of high importance to an organization, such as `MSExchangeIS`, which will make Exchange content inaccessible (Citation: Novetta Blockbuster). In some cases, adversaries may stop or disable many or all services to render systems unusable.(Citation: Talos Olympic Destroyer 2018) Services or processes may not allow for modification of their data stores while running. Adversaries may stop services or processes in order to conduct [Data Destruction](<https://attack.mitre.org/techniques/T1485>) or [Data Encrypted for Impact](<https://attack.mitre.org/techniques/T1486>) on the data stores of services like Exchange and SQL Server.(Citation: SecureWorks WannaCry Analysis)

Country

Name

Ukraine

Region

Name

Eastern Europe

Name

Europe

Sector

Name

Telecommunications

Description

Private and public entities involved in the production, transport and dissemination of information and communication signals.

Domain-Name

Value

solntsepek.ru

solntsepek.org

solntsepek.info

solntsepek.com

IPv4-Addr

Value

185.61.137.155

StixFile

Value

6a8824048417abe156a16455b8e29170f8347312894fde2aabe644c4995d7728

External References

-
- <https://www.sentinelone.com/labs/acidpour-new-embedded-wiper-variant-of-acidrain-appears-in-ukraine/>
-
- <https://otx.alienvault.com/pulse/65fc916967e188b26fe41f0b>