



# BRANDEFENSE

CYBER THREAT INTELLIGENCE

## SandWorm APT Group Cyber Intelligence Report

Author: Threat Intelligence Team

Date: 30.05.2022

Report ID: SAPTGCIR15042022



## Executive Summary

---

The Russian state-supported Sandworm APT group is discussed in this report prepared by the Brandefense threat intelligence team. APT's objectives, motivations, past cyberattacks, which started in 2009, group's Tactics, Techniques, and Procedures (TTPs), malwares, open-source tools, IoC findings, and YARA rules explained in this report.

Cyber attack methods and malware investigations in this report will create cyber security awareness. In addition, TTP findings and IoC datas used by threat actors will contribute by feeding cybersecurity teams and products.


Correct understanding of Tactics, Techniques, and Procedures used by the threat group and their utilities/malwares and it's capabilities will provide a proactive approach for to future attacks and will enable the necessary steps to be taken to take early action.

Considering the report's general scope and content, it aims to nurture rule-based security solutions together with network and machine-based security solutions and to be illuminating in terms of raising security awareness against targeted cyber attacks.

# Introduction



Sandworm APT Group Overview

Reference Names	Sandworm Team (Trend Micro) Iron Viking (SecureWorks) CTG-7263 (SecureWorks) Voodoo Bear (CrowdStrike) Quedagh (F-Secure) TEMP.Noble (FireEye) ATK 14 (Thales) BE2 (Kaspersky)
Country	 Russia
Sponsor	State-sponsored, GRU Unit 74455
First Seen	2009
Motivation	Sabotage && Espionage
Method	Zero-days, Malware, Spearphishing
Targeted Industries	Education, Energy, Government, Telecommunications

Sandworm Team, also known as Unit 74455, is a Russian cyberespionage group operating since 2009. The group is allegedly affiliated with the cyber military unit of the Main Intelligence Service (GRU), which is working for Russian military intelligence.

Sandworm Team mainly targets Ukrainian organizations associated with energy, industrial control systems, SCADA, government, and media sector.

Sandworm Team was directly linked to the Ukrainian energy sector attack in late 2015.

# SandWorm's History and Motivation



## SandWorm's History and Motivation

### Sandworm APT Targets Windows 0-day Vulnerabilities

A critical zero-day vulnerability in the Windows operating system has been found by the Sandworm APT group to have been used against NATO, Ukrainian government agencies, several Western European government agencies, companies operating in the energy sector, and European telecommunications companies. It used Black Energy backdoor malware in Sandworm attacks, which exploited the vulnerability for cyber espionage.

October 2014



### Ukrainian Cities Hit With Blackouts after Cyberattacks

In Ukraine's Ivano-Frankivsk Oblast, there was a power outage that affected the entire region. Studies have shown that the utility has started disconnecting power substations for no apparent reason. A malware attack was carried out, and the "remote management system" (SCADA and EMS systems) was taken out of service. It was announced that the blackout continued in the entire region for 6 hours, and the attack was associated with the Sandworm APT group.

December 2015



### Centreon Supply Chain Attack by Sandworm APT Group

Targeting Centreon monitoring software, Sandworm launched an attack campaign against French organizations that resulted in a data breach.

December 2017



### Critical Vulnerability in Exim Targeted by Sandworm Group

Sandworm APT group carried out attacks by taking advantage of the security weakness detected in Exim (MTA) software for about one year.

August 2019



### Russian GRU Officers Associated with Sandworm APT Group

Six different Russian GRU officials were accused of organizing malware campaigns as part of the Sandworm APT group.

October 2020





## SandWorm's History and Motivation

---

### Motivation

The GRU or GU (General Staff of the Armed Forces of the Russian Federation) is a military foreign intelligence agency. Sandworm APT operates within this intelligence agency; It has advanced and disruptive capabilities to conduct global disinformation, propaganda, espionage, and cyber operations.

GRU, had previous cyber operations against Estonia in 2007 and Georgia in 2008, has become more visible with the recent cyber operations. Western intelligence agencies attributed the last significant attacks to this agency. While it is difficult to assess whether the GRU is taking a leading role among other special services in conducting operations in cyberspace, it has serious activities.

GRU has capabilities focused on improving both technical and psychological capabilities. For example, the 85th Special Service Center (Unit 26165) and Special Technologies Headquarters (Unit 26165), traditionally responsible for signal intelligence and cryptography, have been responsible for computer-based operations. The 72nd Special Service Center (Unit 54777), which forms the core of the GRU's psychological warfare team, has been working closely with 'technical' units and carrying out cyberattacks through frontline organizations since at least 2014.

Unit 74455 (Sandworm) is credited with creating and distributing malware used for spoofing operations during the 2016 US Presidential election, the NotPetya malware, and Ukraine's electrical infrastructure attacks.



Russia's security agencies are in competition with each other and often carry out similar operations on the same targets. Therefore, it becomes difficult to make specific attribution and motivational assessments. However, in some cases, attacks can also be carried out jointly. For example, some of the Sandworm APT group's attacks were carried out with the help of GRU Unit 26165, the Russian GRU cyber military unit that is part of Fancy Bear (APT28).

On the next page, the special services of Russia involved in cyber operations and the threat groups connected to these services were shared.



SandWorm’s History and Motivation

Russian Special Services Involved in Cyber Operations

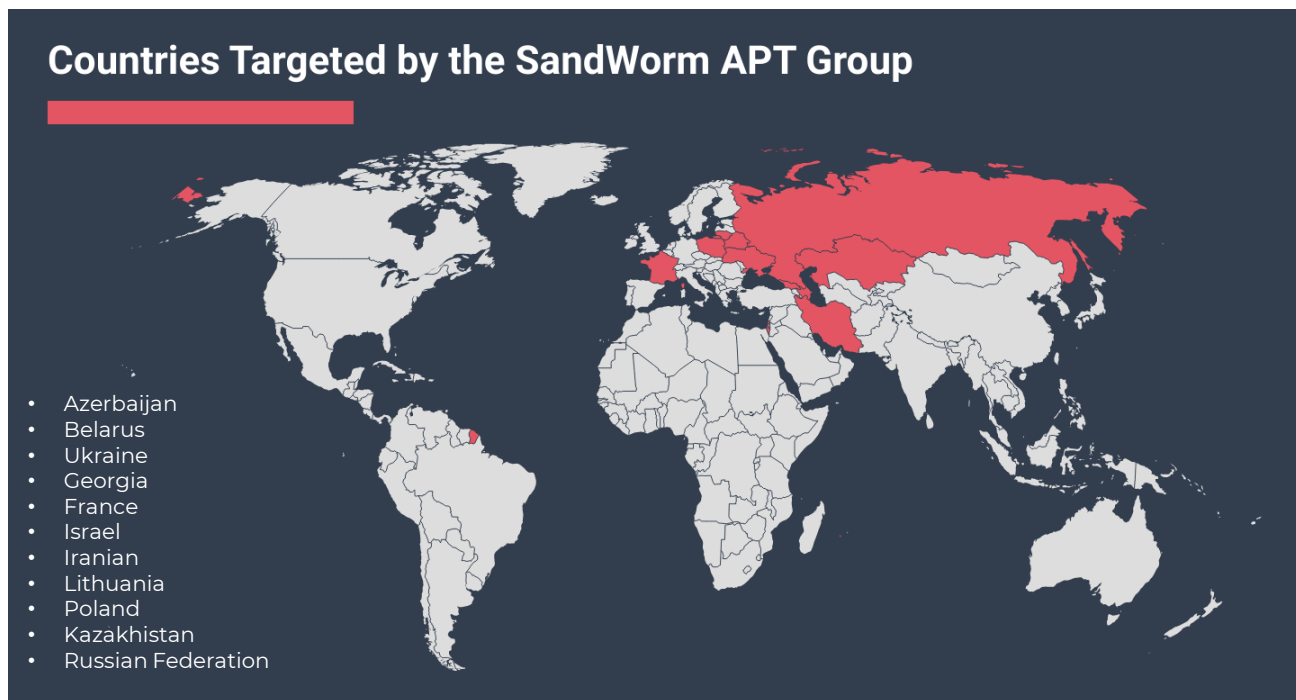
Service	Group	Targeted Countries
 <p>• <b>GRU/GU</b></p> <p>• Main Intelligence Service of the Armed Forces of Russia</p>	<ul style="list-style-type: none"><li>• SandWorm</li><li>• APT 28</li><li>• CyberBerkut</li><li>• CyberCaliphate</li></ul>	<ul style="list-style-type: none"><li>• Ukraine</li><li>• America</li><li>• France</li><li>• Germany</li><li>• Georgia</li><li>• Montenegro<ul style="list-style-type: none"><li>• India</li><li>• Japan</li><li>• Turkey</li></ul></li><li>• Azerbaijan</li></ul>
 <p><b>FSB</b></p> <p>Federal Security Service</p>	<p>Turla APT (Snake, Uroburos, Waterbug, Venomous Bear)</p>	<p>Algeria Brazil France Germany India Iranian Kazakhstan Latvia Mexican Poland Saudi Arabia SA</p>
 <p><b>SRV</b></p> <p>Foreign Intelligence Service</p>	<p>APT 29 (Cozy Bear, Office Monkeys, Duke, CozyDuke, CozyCar)</p>	<p>Belgium Brazil Chinese Turkey Mexican Ukraine USA Romania Georgia Japan</p>



# Countries and Sectors Targeted by The SandWorm



## Countries and Sectors Targeted by the SandWorm



Sandworm threat actors target industrial control systems associated with electricity and power generation for espionage, decommissioning, and data destruction.

On October 15, 2020, the USA accused 6 GRU personnel associated with the Sandworm Team of conducting the following cyber operations:

- Attacks on Ukrainian electricity companies and state institutions in 2015 and 2016,
- The worldwide NotPetya attack in 2017,
- Hacking of Emmanuel Macron's election campaigns before the 2017 French presidential election,
- Distribution of Olympic Destroyer malware targeting the 2018 Winter Olympic Games,
- 2018 operation against the Organization for the Prohibition of Chemical Weapons,
- Attack on Georgia in 2018 and 2019.

# Tools Used by the SandWorm and Associated Malwares



## Tools Used by the SandWorm and Associated Malwares

Tools/Softwares used	Definition
BlackEnergy	BlackEnergy is a malware toolkit frequently used by the Sandworm APT group. It has been found to be used since 2007. It was originally designed to create botnets for use in Distributed Denial of Service (DDoS) attacks but has evolved into sophisticated malware with support for various plug-ins. It is also known that this malware was used in cyberattacks against Georgia and targeting Ukrainian energy institutions in 2008. There are variants of BlackEnergy2 and BlackEnergy 3.
CHEMISTGAMES	CHEMISTGAMES is a modular backdoor software distributed by Sandworm Team.
Exaramel for Linux	Exaramel for Linux is a backdoor written in the Go Programming Language, compiled as a 64-bit ELF binary file. The Windows version is tracked separately with the title Exaramel for Windows.
Exaramel for Windows	Exaramel for Windows is a backdoor used to target Windows systems. The Linux version is tracked separately under the heading Exaramel for Linux.
Industroyer	Industroyer is an advanced malware framework designed to manipulate the operating processes of Industrial Control Systems (ICS), especially components used in electrical substations. The Industroyer was used in attacks on the Ukrainian power grid in December 2016. Industroyer is the first known malware specifically designed to target and influence electrical grid operations.
Invoke-PSImage	Invoke-PSImage takes a PowerShell script and embeds the script's bytes into the pixels of a PNG image. An example of use is to embed PowerShell code into an image file using the Invoke-Mimikatz module. For instance, by calling the image file from a macro, PowerShell code will be executed, which will download the macro image and, in this case, leak the passwords.
KillDisk	to render the operating system unbootable. It was first observed as a component of the BlackEnergy malware during the cyberattacks against Ukraine in 2015. KillDisk has since evolved into standalone malware used by various threat actors against some targets in Europe and Latin America; A ransomware component was also included with some KillDisk variants in 2016.
Mimikatz	Mimikatz is a credential collection tool developed to collect Windows logins and passwords stored in clear text.



Tools Used by the SandWorm and Associated Malwares

Tools/Softwares used	Definition
Net	Net utility is a component of the Windows operating system. It is used in command line operations for control of users, groups, services, and network connections. Net has many functions. Most of them have multiple capabilities for the Discovery phase, such as collecting system and network information, moving laterally on SMB/Windows admin shares using «net use» commands, and interacting with services.
NotPetya	NotPetya is malware used by the Sandworm Team in a worldwide attack on June 27, 2017. Although NotPetya appears to be ransomware, its main purpose is to destroy data and disk structures on compromised systems. Additionally, attackers used NotPetya to prevent encrypted data from being recoverable. NotPetya also includes worm-like features to propagate across a computer network using the SMBv1 exploits EternalBlue and EternalRomance.
Olympic Destroyer	Olympic Destroyer is malware used by Sandworm Team against the 2018 Winter Olympics held in Pyeongchang, South Korea. The main purpose of Olympic Destroyer was to render the infected computer systems inoperable. The malware uses various native Windows utilities and API calls to perform its destructive tasks. Olympic Destroyer also has worm-like features to maximize its destructive impact and spread across a computer network.
P.A.S. Webshell	P.A.S. Webshell is a public and multi-functional PHP webshell, in use since at least 2016, that allows remote access and code execution on target's web servers.
PsExec	PsExec is a free Microsoft tool that can be used to execute a program on another computer. IT administrators and attackers frequently use it.
Koadic	Koadic is an open source, publicly available, command line post-exploitation framework and penetration testing tool. Koadic is also capable of generating payloads and handles most of the operations using the Windows Script Host.



## Tools Used by the SandWorm and Associated Malwares

### P.A.S. Webshell

Algorithm	Hash Value
MD5	84837778682450cdca43d1397afd2310
SHA-1	c69db1b120d21bd603f13006d87e817fed016667
SHA-256	893750547255b848a273bd1668e128a5e169011e79a7f5c7bb86cc5d7b2153bc

P.A.S. Webshell was developed in PHP language by a Ukrainian student using the pseudonym 'Profexer'. Webshell, which characteristically has password-based encryption, targeted software called Centreon.

Centreon is software for monitoring applications, networks, and systems. The software, which is also an open source version under the GPL 2.0 license, has also been published as a Virtual Image based on the CENTOS operating system.

On some Centreon servers affected by the attacks, some PHP files containing the source code of version 3.1.4 of P.A.S. Webshell has been detected. It has been seen that the files belonging to Webshell are located in the following directories.

- /usr/local/centreon/www/search.php
- /usr/share/centreon/www/search.php
- /usr/share/centreon/www/modules/Discovery/include/DB-Drop.php
- /usr/share/centreon/www/htmlHeader.php

To the same files over the internet; It has been determined that it can also be accessed using the URL “http://<IP>/centreon/search.php”.

### Webshell Encryption

One of the distinguishing features of malware is that it uses a specific encryption layer. With this feature, it tries to hide its activities by providing anti-analysis. When deployed to a compromised computer, it also uses this layer of encryption to enforce access control.

P.A.S. webshell's PHP file consists of two main parts:

- The main functions that will be executed after activation,
- A form supported by the decryption mechanism to handle the password entered by the operator.



## Tools Used by the SandWorm and Associated Malwares

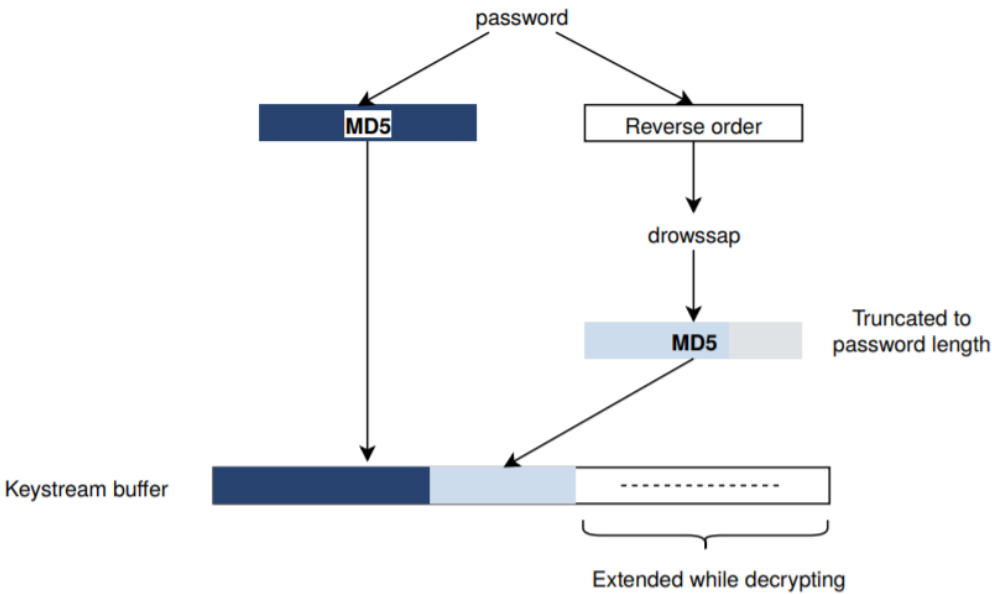
Below is the code snippet of a formatted and deobfuscated version of Webshell.

```
$password=isisset($_POST['password'])?$_POST['password']:(isset($_COOKIE['password'])?
→$_COOKIE['password']:NULL);

if($password!=NULL)
{
$password=md5($password).substr(MD5(strrev($password)),0,strlen($password));
for($counter=0;$counter<15571;$counter++)
{
$webshell_data[$counter]=chr((ord($webshell_data[$counter])-
→ord($password[$counter]))%256);
$password.=$webshell_data[$counter];
}

if($webshell_data=@gzinflate($webshell_data))
{
if(isset($_POST['password']))
@setcookie('password'$_POST['password']);
$counter=create_function(''$webshell_data);
unset($password$webshell_data);
$counter();
}
}
```

When the decryption mechanism is examined, a decryption keystream buffer is created using the MD5 hash value of the password. The generated value is concatenated with a second value with the MD5 hash in reverse order of the password and truncated to the length of the password.



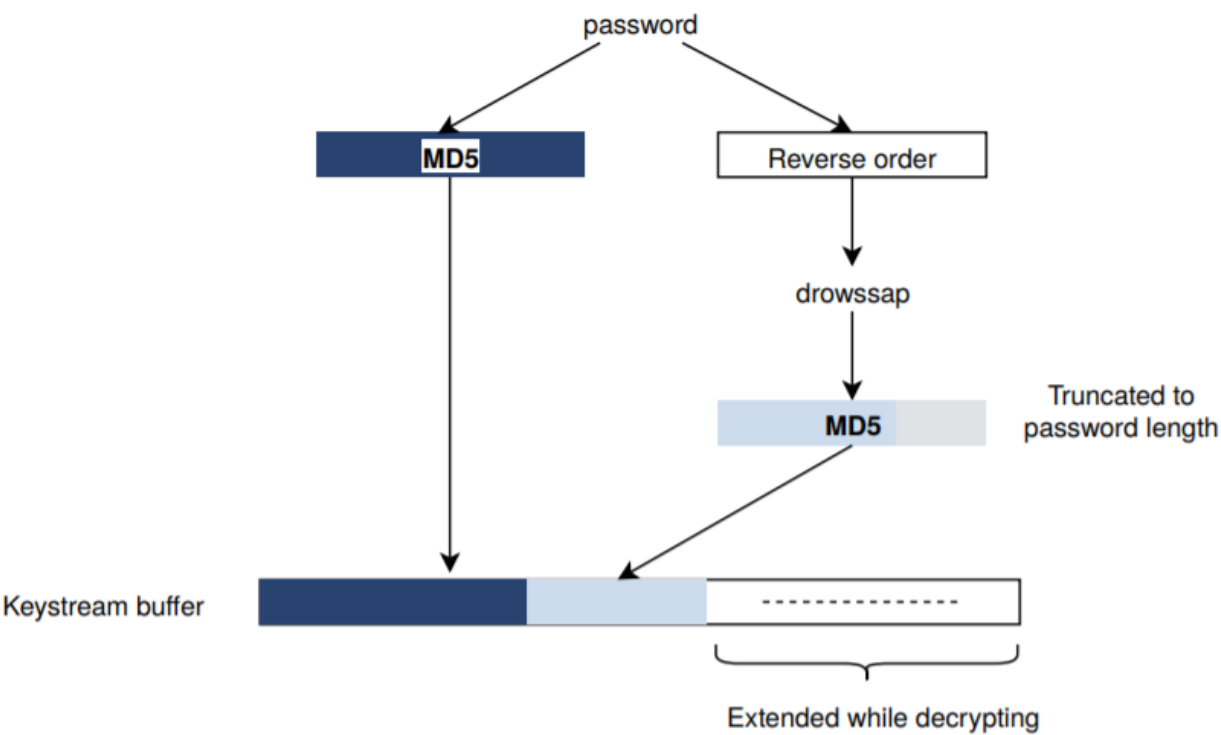
P.A.S. Generating the Decryption Key



Tools Used by the SandWorm and Associated Malwares

Decryption Mechanism

Decryption Keystream Buffer is generated using the MD5 hash value of the password. The generated value is sorted in reverse order of the password and combined with a second value from the MD5 hash value, and shortened to the length of the password.



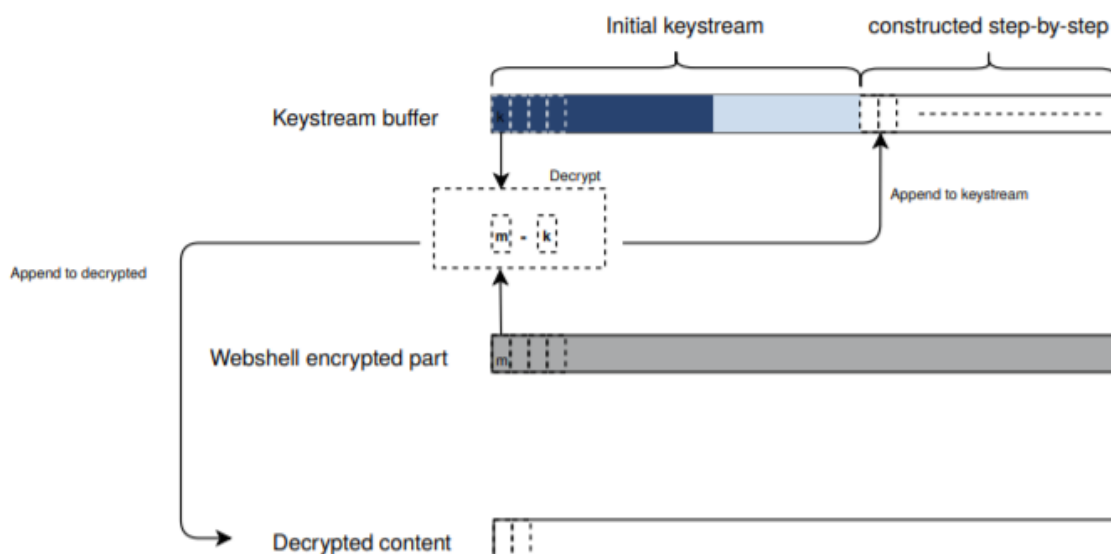
P.A.S. Decryption Key Generation



## Tools Used by the SandWorm and Associated Malwares

The program then enters a loop where for each iteration, a character from the Decryption Key Buffer is extracted from one byte of the encrypted Webshell. The result obtained is used both as the decrypted data and added to the Key Buffer. Thus, the Keystream is created.

In the final step, the decrypted Buffer is passed to PHP's gzinflate function for the Uncompress process.



P.O.V Decryption Cycle

## Panel Features

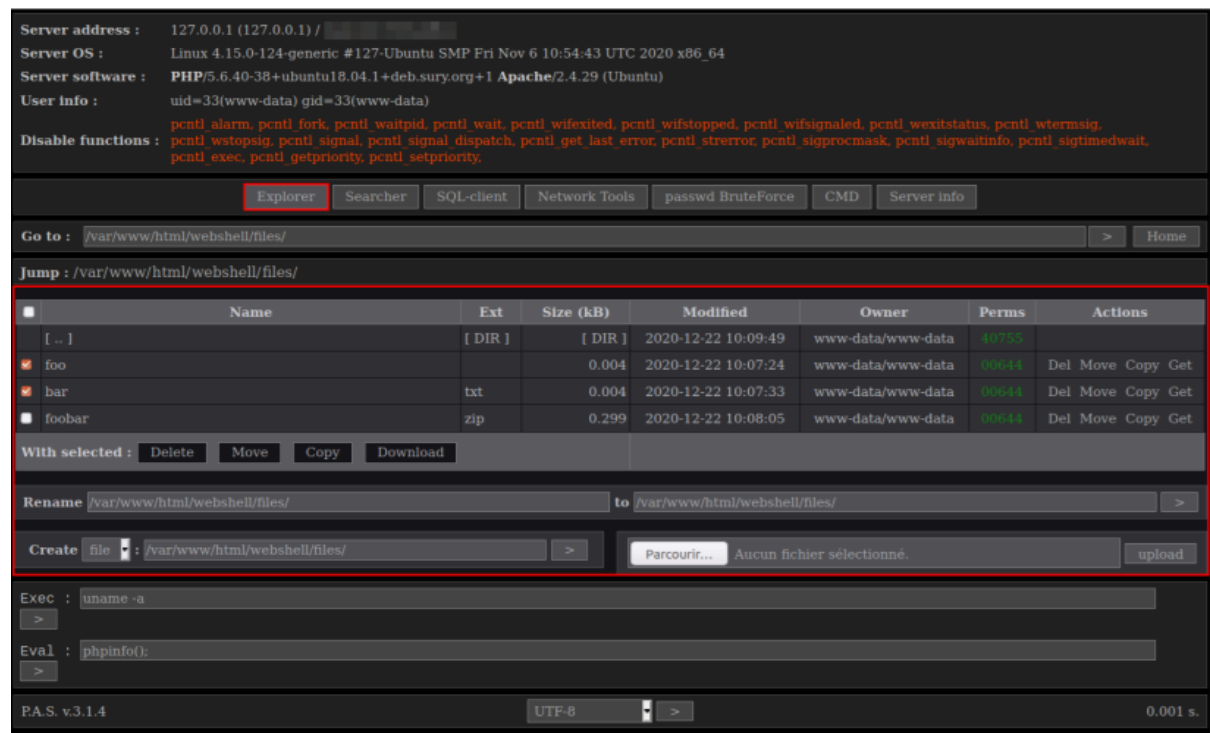
P.A.S. Webshell has various functions grouped according to categories in the submenus in its interface. The malware is installed on the main View. Every function of Webshell is built on a form that aims to get the task parameters before running it and then update the interface to display the results.

The available tabs of the panel are described below.

- **Explorer Menu:** It is the tab used to view, delete, edit, download existing files or upload files to the victim's computer.
- **Searcher Menu:** A tab that searches for specific items in the file system of the compromised computer.



Tools Used by the SandWorm and Associated Malwares



SQL-client Menu

It is the tab that allows the accessible database tables to be listed by malware. It can interact with MySQL, MSSQL, and PostgreSQL databases.

Network Tools Menu

With this tab, a Bind shell with a listening port can be created, a Reverse shell that takes a remote address as a parameter. Network scans can also be run to find open ports and listening services on a machine.

Passwd BruteForce Menu

With this tab, P.A.S. webshell can perform a brute force attack against SSH, FTP, POP3, MySQL, MSSQL, and PostgreSQL services.

CMD Menu

The CMD menu provides a minimalist interface that allows a specific command to be executed or a PHP script to be run.

Server info Menu

An information screen in the last menu allows a quick collection of information about the compromised computer.



## Tools Used by the SandWorm and Associated Malwares

### Exaramel Backdoor

Algorithm	Hash Value
MD5	8eff45383a7a0c6e3ea6d526a599610d 92ef0aaf5f622b1253e5763f11a08857
SHA-1	F74ea45ad360c8ef8db13f8e975a5e0d42e58732 a739f44390037b3d0a3942cd43d161a7c45fd7e7
SHA-256	C39b4105e1b9da1a9cccb1dace730b1c146496c591ce0927fb035d48e9cb5c0f e1ff729f45b587a5ebbc8a8a97a7923fc4ada14de4973704c9b4b89c50fd1146

Exaramel is a Backdoor malware that was first detected in 2018. Two samples were identified, one targeting the Windows operating system and the other targeting the Linux operating system. The version targeting Linux appeared to be uploaded to the Virustotal platform in October 2019.

Backdoor named “centeron\_module\_linux\_app64” is detected in Centreon server folders ‘/usr/share/centreon/www/’ and ‘/usr/local/centreon/www/modules/'. In the same folder, a script named respawner.sh, config.json,configtx.json config files, and a few other files named with the .rep extension were seen.

From November 2017 to February 2018, logs were encountered showing the respawner.sh file is executed daily by Cron.

### Technical Analysis

Exaramel is written in the GO programming language, and the source code consists of approximately 1400 lines. The malware is divided into five main packages: main, worker, config, scheduler, and networker.

Alongside the standard GO library, Exaramel has been seen using two more open source packages:

- [github.com/robfig/cron](https://github.com/robfig/cron)
- [github.com/satori/go.uuid](https://github.com/satori/go.uuid)

The important variables in the source code are listed below.

- **\$EXARAMEL\_DIR:** The folder where Exaramel was written.
- **\$EXARAMEL\_PATH:** The full path to the Exaramel binary.
- **\$EXARAMEL\_GUID:** The UUID field of the Exaramel configuration.
- **\$SERVER\_URL:** Exaramel Command Control URL.
- **\$DEFAULT\_SERVER\_IP:** The command and control IP address used in the default configuration.



## Tools Used by the SandWorm and Associated Malwares

---

Exaramel is a remote management tool that supports multitasking. It has functions such as copying files from the command control server to the Exaramel infected computer, sending files from the victim computer to the command and control server, and executing shell commands.

Exaramel communicates with the command and control server using HTTPS to get the list of tasks it needs to run. Then it continues its activities with different methods.

Exaramel's working mechanism can be divided into two parts: Initialisation and Main Loop.

### Initialisation

Exaramel creates a UNIX socket named '/tmp/.applocktx'. This socket is not used to communicate but only to prevent Exaramel from executing concurrently. If socket creation fails, Exaramel stops execution, with an error message stating that the local address is already in use (App has already started!).

Exaramel creates a handler for SIGINT, SIGTERM, SIGQUIT and SIGKILL signals. The Handler's job is to terminate the Exaramel process.

Exaramel reads the configuration file.

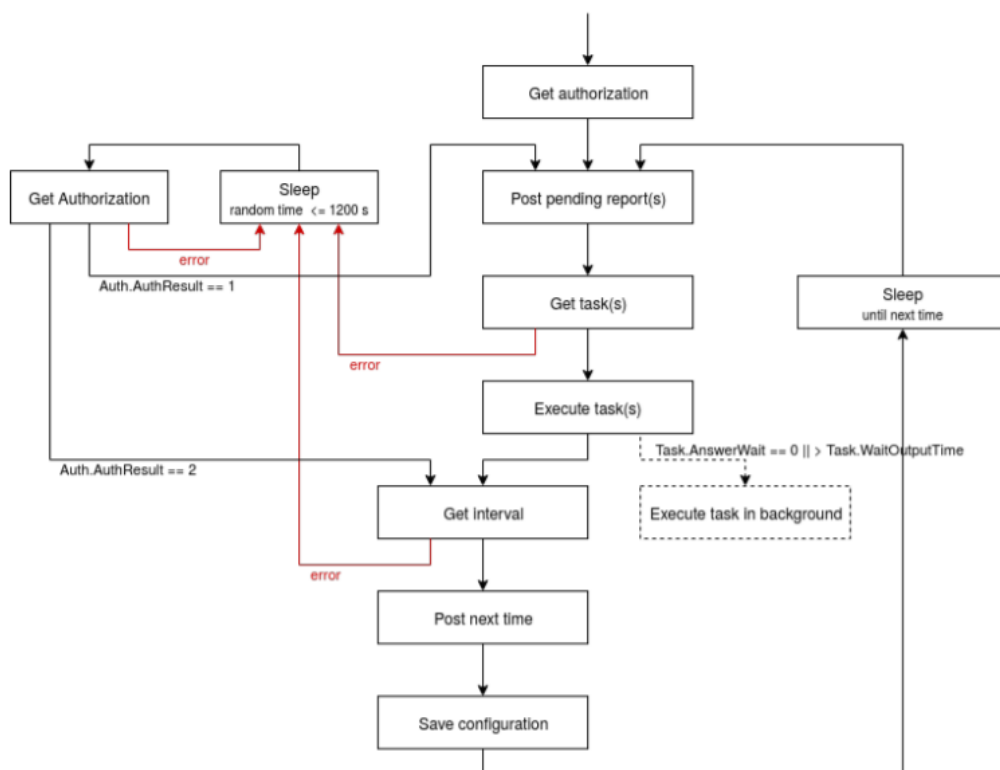
Exaramel checks if a persistence method is enabled. If it is not enabled, it uses various techniques to ensure persistence.

### Main Loop

The main cycle can be summarized in four steps:

1. Exaramel contacts the command and control server to get a list of tasks to execute.
2. Exaramel runs the tasks it receives. Some can run in the background indefinitely.
3. Exaramel communicates with the command and control server to get the interval of time it should suspend before connecting to the server.
4. Exaramel suspends itself until the set time is up.

## Tools Used by the SandWorm and Associated Malwares



## Configuration

Exaramel stores its configuration in a file named 'configtx.json' in the \$EXARAMEL\_DIR folder. This file is encrypted using the RC4 algorithm and the key 'odhyrfjcnfkdtstlt'. The resulting file after decryption is in JSON format. Its specification in GO language is given below.

```

Config struct{
    //URLs server list
    Hosts[]string
    //Proxy HTTP URL to connect to servers (optional)
    Proxy string
    //EXARAMEL version
    Version string
    //UUID used probably to identify an Exaramel instance
    Guid string
    //Timespan of the last run pause between two mails loop run.
    //This field is updated before each execution pause.
    Next int64
    //Date when EXARAMEL last paused its execution
    Datetime string
    //Timeout value given to HTTP/HTTPS implementation
    Timeout int
    //Time during which EXARAMEL paused its execution between two
    //main loop iterations. This field is used when EXARAMEL
    //fails to get a time interval from its control server.
    Def int64
}
    
```



## Tools Used by the SandWorm and Associated Malwares

Exaramel starts reading the configuration file during the Initialisation phase. If it fails, it uses its default configuration and creates a new configuration file. The default configuration is as follows.

```
{
  "Hosts":["https://$DEFAULT_SERVER_IP/api/v1"]
  "Proxy":""
  "Version":"1"
  "Next":20
  "Datetime":""
  "Timeout":30
  "Def":20
}
```

The GUID field is created with the UUID GO package when using the default configuration. The configuration is rewritten to the same file at the end of the main loop. This file is also deleted when Exaramel deletes itself.

### Get Tasks

Exaramel sends a GET request to \$SERVER\_- URL/tasks.get/\$EXARAMEL\_GUID to receive new tasks from the Command and Control server. Both servers are expected to respond in the corresponding Json with a Tasks or RespError construct.

```
Tasks struct{
  // Liste de tâches
  Response []TaskResponse `json:"response"`
}
type TaskResponse struct{
  // Task identification
  ID uint32 `json:"id"`
  // Task type, e.g. "OS.ShellExecute" or "IO.ReadFile"
  Method string `json:"metod"`
  // Optional argument needed for some tasks
  Arguments string `json:"arguments"`
  // Not used
  Attachment int `json:"attachment"`
  // Only for "OS.ShellExecute" task. If the field is non zero, the shell process
  // will be run in the background.
  AnswerWait int `json:"answer_wait"`
  // No real impact in task processing
  DoAsync int `json:"answer_async"`
  // If the field is non zero, the report will be sent as soon as the task ends
  AnswerImmediately int `json:"answer_immediately"`
  // Max task duration. Once it is reached the task
  // is left in the background and a report is produced.
  WaitOutputTime int `json:"wait_output_time"`
}
```

# SandWorm APT MITRE ATT&CK Mapping



MITRE ATT&CK Mapping

MITER ATT&CK is an open knowledge base of techniques, tactics, and procedures used by threat actors. By observing the attacks that occur in the real world, the behavior of threat actors is systematically categorized.

With MITER ATT&CK, it is aimed to determine the risks against the actions that the threat actors can take in line with their targets and make the necessary improvements and plans.

The following Mitre ATT&CK Threat Matrix has been created to provide information on the techniques, tactics, and procedures used by Sandworm APT.

Tactic ID	Tactic	Technique ID	Technique
TA0043	Reconnaissance	T1595 T1592 T1589 T1590 T1591 T1598 T1593 T1594	Active Scanning Gather Victim Identity Information Gather Victim Identity Information Gather Victim Identity Information Gather Victim Identity Information Phishing for Information Search Open Websites/Domains Search Victim-Owned Websites
TA0042	Resource Development	T1583 T1585 T1588	Acquire Infrastructure Establish Accounts Obtain Capabilities
TA0001	Initial Access	T1133 T1566 T1199 T1078	External Remote Services Phishing Trusted Relationship Valid Accounts
TA0002	Execution	T1059 T1203 T1204 T1047	Command and Scripting Interpreter Exploitation for Client Execution User Execution Windows Management Instrumentation
TA0003	Persistence	T1098 T1136 T1133 T1505 T1078	Account Manupilation Create Account External Remote Services Server Software Component Valid Accounts
TA0003	Privilege Escalation	T1078	Valid Accounts





MITRE ATT&CK Mapping

Tactic ID	Tactic	Technique ID	Technique
TA0005	Defense Evasion	T1140 T1562 T1070 T1036 T1027 T1218 T1078	Deobfuscate/Decode Files or Information Impair Defenses Indicator Removal on Host Masquerading Obfuscated Files or Information Signed Binary Proxy Execution Valid Accounts
TA0006	Credential Access	T1110 T1555 T1056 T1040 T1003	Brute Force Credentials from Password Stores Input Capture Network Sniffing OS Credential Dumping
TA0007	Discovery	T1087 T1083 T1040 T1018 T1082 T1016 T1049 T1033	Account Discovery File and Directory Discovery Network Sniffing Remote System Discovery System Information Discovery System Network Configuration Discovery System Network Connections Discovery System Owner/User Discovery
TA0008	Lateral Movement	T1570 T1021	Lateral Tool Transfer Remote Services
TA0009	Collection	T1005 T1056	Data from Local System Input Capture
TA0011	Command and Control	T1071 T1132 T1105 T1571 T1090 T1219 T1102	Application Layer Protocol Data Encoding Ingress Tool Transfer Non-Standard Port Proxy Remote Access Software Web Service
TA0010	Exfiltration	T1041	Exfiltration Over C2 Channel
TA0040	Impact	T1485 T1491 T1561 T1499	Data Destruction Defacement Disk Wipe Endpoint Denial of Service



## MITRE ATT&CK Mapping

---

### **T1566: Phishing**

The SandWorm threat group primarily uses targeted phishing e-mails to gain access to computers or account credentials. Phishing specially prepares e-mails to appear as if they are from trusted people/institutions. Attackers have gone so far as to develop and test spearphishing techniques before executing their campaigns to increase their chances of success.

### **T1059: Command and Scripting Interpreter**

SandWorm uses PowerShell commands and scripts to discover system information, execute code, and download malware. In addition, the group ran a PowerShell script by distributing malware with a credential collection tool. However, since the tool only works in memory, it was not easily detected by antivirus software.

### **T1204: User Execution**

Most spear phishing emails sent by SandWorm contained malicious documents. If the user executes the malicious document, the attackers get the initial access.

### **T1078: Valid Accounts**

To maintain its persistence, SandWorm collects and reuses the credentials of existing accounts on victim systems. The group was widely seen using malware to maintain control over victim computers and networks and increase their authority over the system. It also used related malware to elevate system privileges and determine if specific antivirus processors were working. The final step of the attack was seen using legitimate credentials to leak data from the victim's network and extract internal documents from machines in victim environments.

### **T1070: Indicator Removal on Host**

SandWorm used a proprietary algorithm to hide certain features of the Olympic Destroyer malware to block post-attack analysis and avoid detection. The group has also tried to hide their activity by clearing the event logs and deleting data from compromised machines and servers.

### **T1036: Masquerading**

SandWorm has been trying to hide its activities by imitating malware used by the Lazarus group.

### **T1003: OS Credential Dumping**

The SandWorm group was found to collect accounts and credentials from compromised machines.



## MITRE ATT&CK Mapping

---

### **T1552: Unsecured Credentials**

SandWorm used specialized malware to collect any additional usernames and passwords it could obtain from the previous computer before spreading to the next computer.

### **T1210: Exploitation of Remote Services**

SandWorm has attacked remote services of targets to gain unauthorized access over the internal network. After gaining access to the remote system, they deployed malware in an attempt to gain system privileges, move laterally across the network, and execute an open source credential collection tool.

### **T1083: File and Directory Discovery**

SandWorm threat actors search the system for files containing credentials and network configuration details on compromised machines. After gaining access to victims' computers, it also performed various functions designed to identify, collect, package, and display targeted data, including usernames, IP addresses, and server data related to RDP sessions on target computers. The related malware has been seen in many cases where it aims and is used for obtaining credentials that allow victims to move laterally and exponentially across computer networks.

### **T1001: Data Obfuscation**

SandWorm creates a command and control server to enable communication between compromised networks and a server they control. The created tunnel allows them to hide their activity, run commands, install additional tools, and transfer data.

### **T1491: Defacement**

SandWorm hacked the Georgia-based web hosting provider, hijacking nearly 1,500 websites, disrupting service to some of these websites.

### **T1490: Inhibit System Recovery**

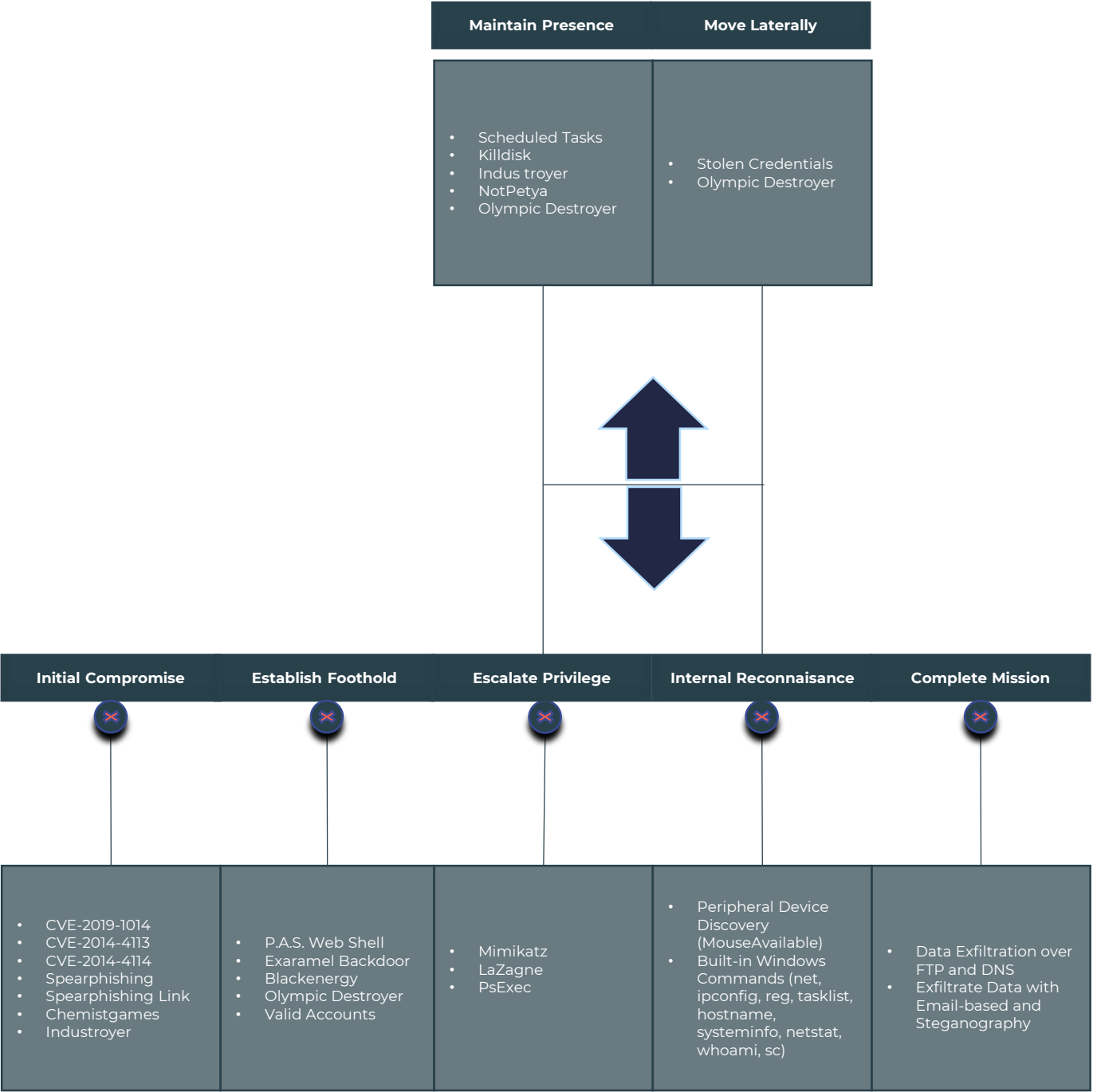
SandWorm has distributed destructive malware to delete files on the hard drive, shut down the computer, misconfigure BitLocker, render computers inoperable, preventing reboots and recovery.

# Attack Lifecycle and TTP Findings



Attack Lifecycle and TTP Findings

The attack life cycle of the Sandworm APT group is examined in the table below. In addition, the tools, vulnerabilities, technical tactics, and procedures used by the group in attacks are included.



# Critical Attacks by Sandworm APT Group

## Critical Attacks by Sandworm APT Group

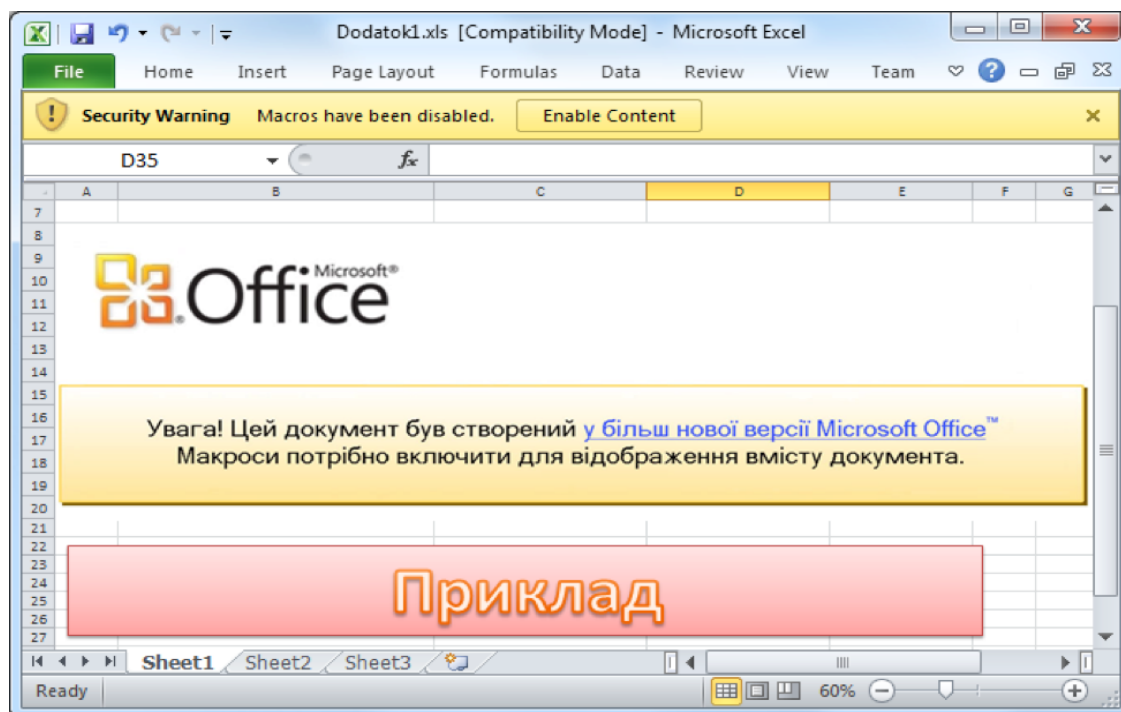
### BlackEnergy Attacks Targeting the Electricity Industry in Ukraine

BlackEnergy is a trojan used to carry out cyber espionage and information destruction attacks. In 2014, BlackEnergy (Sandworm) threat actors started to distribute malware affecting SCADA/ICS systems to targets in energy markets worldwide.

#### Technical Analysis

Since mid-2015, the BlackEnergy APT group has actively used spear-phishing emails carrying malicious Excel documents with macros to infect computers on a targeted network. However, in January 2015, a new malicious document was discovered that infected the system with a BlackEnergy trojan. Unlike Excel documents used in previous attacks, a Microsoft Word document has been detected. After opening the document, the user is presented with a dialog suggesting that macros must be enabled to view the content. Enabling macros triggers BlackEnergy malware infection.

In these attacks against electricity distribution companies in Ukraine, it was observed that a destructive KillDisk malware was downloaded and executed on the systems infected by the BlackEnergy trojan. And as a result of the attacks, on December 23, 2015, half of the settlements in Ukraine's Ivano-Frankivsk region (approximately 1.4 million inhabitants) suffered a power outage for several hours.





## Critical Attacks by Sandworm APT Group

---

### Attacks via NotPetya Worm

In June 2017, it was reported that a number of Ukrainian banks and Ukrainian state electricity distributor Ukrenergo were affected by unidentified malware that caused significant operational disruptions. The malware was later identified by multiple security vendors and independent researchers as a type of Ransomware with functional and technical similarities to Petya and worm capabilities. Based on these similarities and ongoing confusion, the malware has been named Nyetya, Petna, ExPetr, and NotPetya. NotPetya attacks, which have been associated with numerous infections affecting machines in Ukraine, have been attributed by security researchers, Google, and various governments to the Sandworm APT group within the GRU Russian military intelligence agency.

Notpetya was detected while encrypting computers in Ukraine before reportedly infecting systems in Spain, Germany, Israel, the United Kingdom, the Netherlands, and the United States. In addition, the malware has affected several industries, targeting governments, shipping companies, oil companies, and nuclear systems.

### Technical Analysis

NotPetya, which is responsible for locking the infected systems and encrypting all the files inside, is known to spread through the Eternal Blue security vulnerability in Windows systems. The difference between NotPetya from its previous variant, Petya, is that although it looks like traditional ransomware, it encrypts the target's files without recovery after execution.

Due to the NotPetya worm ability, it spreads on its own. Whereas the original Petya spread required the target to download it from a spam email, launch it and grant it administrator permissions. NotPetya uses several different methods to spread without human intervention. As a result of the analysis, it has been observed that the infection vector is a backdoor embedded in MEDoc, an accounting software package used by almost every Ukrainian company. NotPetya, which infects computers from Medoc servers, then takes advantage of EternalBlue and EternalRomance exploits to spread to other systems. Additionally, NotPetya leverages the MimiKatz tool to find network management credentials in the infected machine's memory, then uses the PsExec and WMIC tools built into Windows to remotely access and infect other computers on the local network.





## Critical Attacks by Sandworm APT Group

In summary, Although NotPetya gives the impression of ransomware to the targets, it is a destructive malware whose ultimate goal is to cause permanent damage to the targeted systems. It is clear that the motivation behind the observed attacks is not financial gain. In line with this information, it can be said that NotPetya is a politically motivated cyber weapon deployed by Russia against Ukraine.

```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted. Perhaps you are busy looking for a way to recover your
files, but don't waste your time. Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily. All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

    1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWx

2. Send your Bitcoin wallet ID and personal installation key to e-mail
    wowsmith123456@posteo.net. Your personal installation key:

    74f296-2Nx1Gm-yHQRWr-S8gaN6-8Bs1td-U2DKui-2ZpKJE-kE6sSN-o8tizU-gUeUMa

If you already purchased your key, please enter it below.
Key: _
```

## Spear-phishing Campaigns for the 2017-2018 PyeongChang Winter Olympics

Between December 2017 and February 2018, Sandworm launched spearphishing campaigns and mobile app attacks targeting South Korean citizens, officials, Olympic athletes, partners, visitors, and the International Olympic Committee (IOC). The attacks occurred soon after the Russian athletes were banned from sporting events due to a state-sponsored doping scheme.

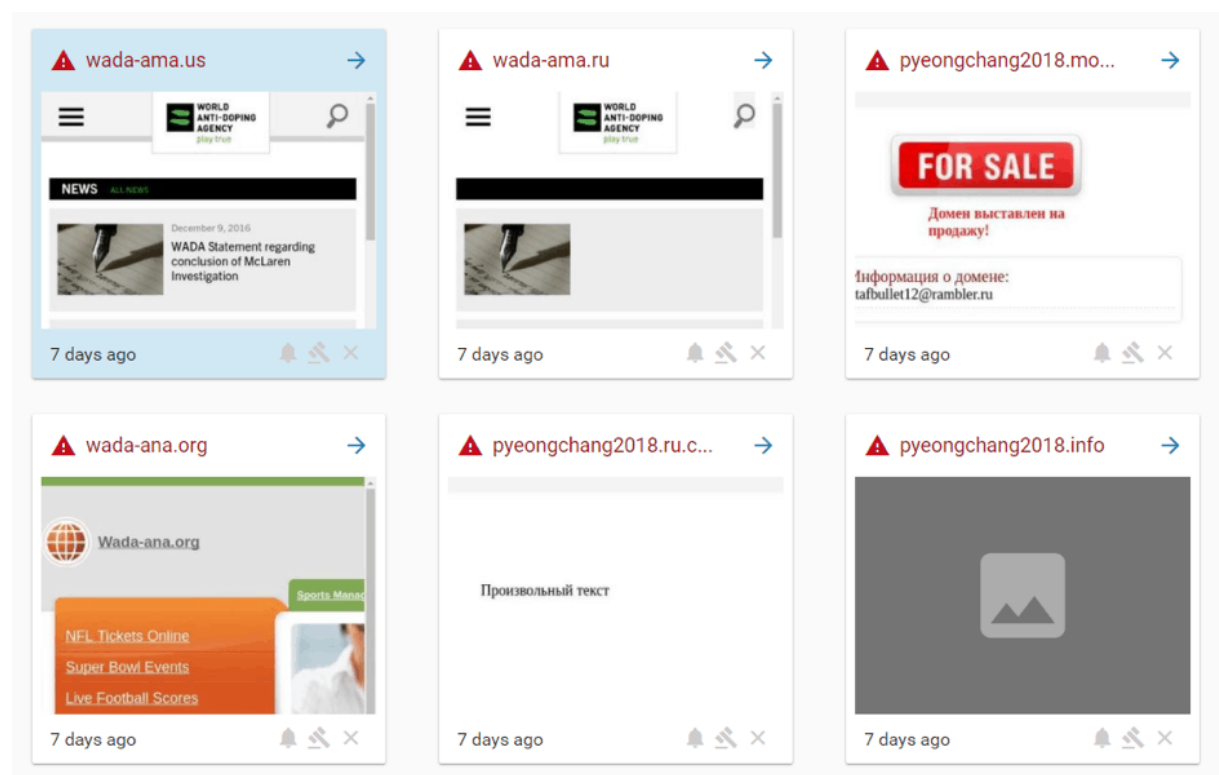
Additionally, in February 2018, Sandworm APT began distributing Olympic Destroyer, a destructive malware strain targeting web servers, during the opening ceremony of the 2018 Winter Olympics. As a result, computers supporting the 2018 PyeongChang Winter Olympic Games, which concluded on February 9, 2018, with the launch of the Olympic Destroyer, were hacked. The organizers of the Pyeongchang Olympics made statements confirming that the malware in question temporarily disabled IT systems, turned off display monitors, and took Wi-Fi and the Olympic website out of service ahead of the official opening ceremonies.



## Critical Attacks by Sandworm APT Group

Between December 2017 and February 2018, Sandworm launched spearphishing campaigns and mobile app attacks targeting South Korean citizens, officials, Olympic athletes, partners, visitors, and the International Olympic Committee (IoC). The attacks took place soon after the Russian athletes were banned from sporting events due to a state-sponsored doping scheme.

Additionally, in February 2018, Sandworm APT began distributing Olympic Destroyer, a destructive malware strain targeting web servers, during the opening ceremony of the 2018 Winter Olympics. As a result, computers supporting the 2018 PyeongChang Winter Olympic Games, which concluded on February 9, 2018, with the launch of the Olympic Destroyer, were hacked. Organizers of the Pyeongchang Olympics made statements confirming that the malware in question temporarily paralyzed IT systems, turned off display monitors, and took Wi-Fi and the Olympic website out of service ahead of the official opening ceremonies.

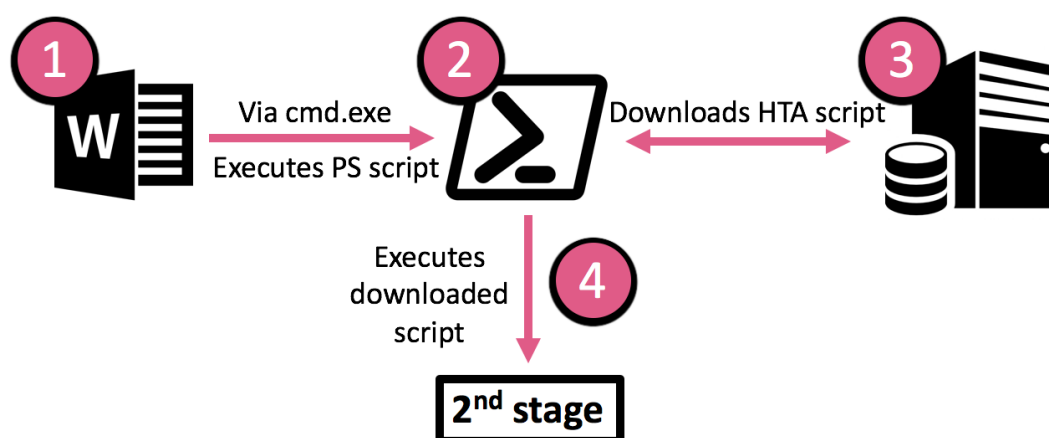


## Critical Attacks by Sandworm APT Group

The chain of attacks begins with distributing malicious MS Office documents via spearphishing e-mails about the Winter Olympics. The documents in question contain gibberish that is lightly formatted to make the text look like it has an encoding problem, and this is a way to get users to enable the "Enable Content" option.

When the target "enables content," the document starts a cmd.exe process to execute a PowerShell script so that the second stage PowerShell script is downloaded, executed, and finally backdoor deployed to the system.

In summary, the networks of official partners of the Winter Olympics were targeted through spearphishing e-mails. In this process, it is assumed that threat actors first use the official website to learn the names of partner companies, identify domain names, and run their campaigns by collecting known e-mail addresses.



## Offensive Campaigns to Sabotage Investigations into Novichok Poisoning

In April 2018, SandWorm thwarted attempts to hold Russia accountable for using a weapons-grade nerve agent on foreign soil by launching phishing campaigns against international and government agencies investigating the poisoning of a former GRU officer and his daughter.

## Critical Attacks by Sandworm APT Group

### Cyber Attacks Targeting Georgia

Sandworm APT carried out cyberattacks in October 2019 that defaced more than 15,000 websites hosted on the infrastructure of Pro-Service, a Georgian web hosting provider, including government sites, local newspapers, and TV stations.

The attack, which is considered the largest cyber attack in the country's history by the local press, affected the sites of various government institutions, banks, courts, local newspapers, and TV stations. The cyberattack in question caused quite a panic in the small Caucasian country.



**WANTED BY THE FBI**

**GRU HACKERS' DESTRUCTIVE MALWARE AND INTERNATIONAL CYBER ATTACKS**

**Conspiracy to Commit an Offense Against the United States; False Registration of a Domain Name; Conspiracy to Commit Wire Fraud; Wire Fraud; Intentional Damage to Protected Computers; Aggravated Identity Theft**

 Yuri Sergeyevich Andrienko	 Sergey Vladimirovich Detistov	 Pavel Valeryevich Frolov
 Anatoliy Sergeyevich Kovalev	 Artem Valeryevich Ochichenko	 Petr Nikolayevich Pliskin

# Conclusion



## Conclusion

---

Analysis of Sandworm APT group and explained findings that can be used by people who work in the information technology departments, who are part of the cyber security team, who have gained competence in areas such as security researchers, system administrators, the following topics are included, are shared:

- ✓ Mission, vision and historical development of Sandworm APT group,
- ✓ Countries and sectors targeted by the group,
- ✓ Cyber attacks carried out by the group,
- ✓ Attack lifecycle and Technical, Tactical, Procedure (TTP) analysis,
- ✓ Tools and malware used by the group in attacks,
- ✓ Precautions/recommendations to be taken for APT attacks,
- ✓ Indicator of Compromise (IoC) findings,
- ✓ Advices

Implementing cyberattack surface management for critical infrastructures targeted by the Sandworm APT group will benefit the organization's access to security maturity.

# Recommendations



## Recommendations

---

Sandworm APT analysis, and group's methods used in their initial access to target systems and the spread process after gaining access are discussed.

When the encountered cases were examined, it was seen that the group mostly used phishing attacks to gain initial access and took advantage of the vulnerabilities in the existing systems. In this context, precautions should be taken by considering the attack vectors used to be protected from attacks that Sandworm APT may carry out. Important recommendations to be implemented to protect assets in the digital world and minimize the risk of exploitation arising from security vulnerabilities and device configuration are shared below.

- An integrated cyber defense platform should be used that shares threat data from email, web, cloud applications, and infrastructure.
- Make sure that multi-factor authentication is enabled for all accounts using your network.
- Internet dependency should be minimized for all critical systems, and control system devices should not be connected directly to the Internet.
- All unused legacy applications should be removed from all machines on the network to avoid abuse.
- Critical networks, such as control system networks behind firewalls, must be isolated from the external network.
- If remote access is required, secure methods such as VPN should be used.
- Unused system accounts should be removed, disabled, or renamed.
- To not be affected by known security vulnerabilities, updates that patch the vulnerabilities should be applied as soon as possible.
- Policies that require the use of strong passwords should be implemented.
- Organizations should keep backups of important data, systems, and configurations.
- The restoring capacity should be tested. Ensure that the restore capabilities support the needs of the business.
- Institution/Organization personnel should be trained to understand cybersecurity principles and not engage in behavior that could compromise network security.





## Recommendations

---

- It aims to create a sense of trustworthiness for its targeted users by imitating a reliable source of threat actors. Therefore, it is recommended that the institution's employees be made aware of current threats of phishing attacks carried out with e-mail content.
- It is highly recommended to prevent IoC findings such as up-to-date attack methods, malware hash values, IP, Domain, and URL addresses involved in malicious/suspicious activities from corporate networks. Thanks to the integration of such a threat list with security devices, IoC findings with verified sources and threat and risk scoring provide a high level of protection against potential threats.

Indicator of  
Compromise



Indicator of Compromise (IoCs)

Table 1: BlackEnergy

Hash (SHA-1)	Description
4c424d5c8cfedf8d2164b9f833f7c631f94c5a4c	Lite Dropper
896fcacff6310bbe5335677e99e4c3d370f73d96	Dropper
069163e1fb606c6178e23066e0ac7b7f0e18506b	Drivers
0b4be96ada3b54453bd37130087618ea90168d72	Drivers
1a716bf5532c13fa0dc407d00acdc4a457fa87cd	Drivers
1a86f7ef10849da7d36ca27d0c9b1d686768e177	Drivers
1cbe4e22b034ee8ea8567e3f8eb9426b30d4affe	Drivers
20901cc767055f29ca3b676550164a66f85e2a42	Drivers
2c1260fd5ceaef3b5cb11d702edc4cdd1610c2ed	Drivers
2d805bca41aa0eb1fc7ec3bd944efd7dba686ae1	Drivers
4bc2bbd1809c8b66eecd7c28ac319b948577de7b	Drivers
502bd7662a553397bbdcfa27b585d740a20c49fc	Drivers
672f5f332a6303080d807200a7f258c8155c54af	Drivers
84248bc0ac1f2f42a41cffa70b21b347ddc70e9	Drivers

Table 2: KillDisk components

Hash (SHA-1)	Description
16f44fac7e8bc94eccd7ad9692e6665ef540eec4	KillDisk
8ad6f88c5813c2b4cd7abab1d6c056d95d6ac569	KillDisk
6d6ba221da5b1ae1e910bbeaa07bd44aff26a7c0c425d3e72a	KillDisk

Table 3: General

Hash (SHA-1)	Description
aa67ca4fb712374f5301d1d2bab0ac66107a4df1	XLS document containing macro
72d0b326410e1d0705281fde83cb7c33c67bc8ca	VBS/Agent.AD Trojan
166d71c63d0eb609c4f77499112965db7d9a51bb	Win32/SSHBearDoor.A Trojan



Indicator of Compromise (IoCs)

Table 4: Olympic Destroyer

Hash (SHA-1)	Description
76ab6e2a89c9df04387913983f636999d2241470fc21b32d718e49a55c0014a3	Olympic Destroyer
53a53a483e869c0dca4f1c105fbed6bdf3335d670c36c14e5aabddc56050b7d8	Olympic Destroyer
15def0208d0c18e5177ea1649ca22197b236100523e2af9cece0737fe5c1ff63	Olympic Destroyer
f2b33dbdee8cd78b67bc27140289a82da22eb646dce1c7b9c13e9dae21d985a8	Olympic Destroyer
31e666bc8675018f52243225163631847b337c551ba120ffb23661e6d6b8d56a	Olympic Destroyer
2d431cbc5cf5a1e17cd806234e13648714d831fa54a7f98710629600f9a4f00d	Olympic Destroyer
c86e149b4583f887b8cfe5ab2b90050c4572907d5256b53764d0ed667d1deb9c	Olympic Destroyer
6224837560a95b4677856d012e1d567ebdd15ce06799c5a7720343b9ddb8cd9c	Olympic Destroyer
b861064dd95af4412a3231c77b9d2bdd55107ce410516cba2f31cec2c155ef92	Olympic Destroyer
e6e58454c52704af982ee3706e370fe86ea0af8ac3051678072174f3786e8931	Olympic Destroyer
21116a6a09f44e578b36e7884b8aff4dd96f5dfea7312ff39c5c3e825480617c	Olympic Destroyer
a73fc13f47cef3f9e92841ea48e8e44a27bd938c2f21d7dd2bff8715370220f7	Olympic Destroyer
5e990930ddde3939d1e2e32fdef6aaa868c29d93e0c8ffb7618ecd5522063fad	Olympic Destroyer
be4dd2d468242eb1b19d36b0c9c6cb119c3b10df8f7ae85ac5befdb9a30575d9	Olympic Destroyer



## Indicator of Compromise (IoCs)

---

### IP (C&C Addresses)

- 5.149.254.114
- 5.9.32.230
- 31.210.111.154
- 88.198.25.92
- 146.0.4.74.7
- 188.40.8.72
- 95.216.13.196
- 103.94.157.5

# YARA Rules



## YARA Rules

---

This section contains YARA rules created by various security providers to detect malware thought to be associated with Sandworm APT.

### Detecting webshell P.A.S.

```
rule WEBSHELL_PAS_webshell {  
  meta:  
    author = "FR/ANSSI/SDO (modified by Florian Roth)"  
    description = "Detects P.A.S. PHP webshell - Based on DHS/FBI JAR-16-2029 (Grizzly Steppe)"  
    reference = "https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf"  
    date = "2021-02-15"  
    score = 70  
  strings:  
    $php = "<?php"  
    $strreplace = "(str_replace("  
    $md5 = ".substr(md5(strrev("$  
    $gzinflate = "gzinflate"  
    $cookie = "_COOKIE"  
    $isset = "isset"  
  condition:  
    ( filesize > 20KB and filesize < 200KB ) and  
    all of them  
}
```



## YARA Rules

### Detection of Zip archives created by P.A.S

```
rule WEBSHELL_PAS_webshell_ZIPArchiveFile {
  meta:
    author = "FR/ANSSI/SDO (modified by Florian Roth)"
    description = "Detects an archive file created by P.A.S. for download operation"
    reference = "https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf"
    date = "2021-02-15"
    score = 80
  strings:
    $s1 = "Archive created by P.A.S. v."
  condition:
    $s1 }
```

### Detection of SQL files created by P.A.S.

```
rule WEBSHELL_PAS_webshell_SQLDumpFile {
  meta:
    author = "FR/ANSSI/SDO"
    description = "Detects SQL dump file created by P.A.S. webshell"
    reference = "https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf"
    date = "2021-02-15"
    score = 90
  strings:
    $ = "-- [ SQL Dump created by P.A.S. ] --"
  condition:
    1 of them
}
```





## YARA Rules

### Detection of PERL network scripts generated by P.A.S.

```
rule WEBSHELL_PAS_webshell_PerlNetworkScript {
  meta:
    author = "FR/ANSSI/SDO"
    description = "Detects PERL scripts created by P.A.S. webshell"
    reference = "https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf"
    date = "2021-02-15"
    score = 90
  strings:
    $pl_start = "#!/usr/bin/perl\n$SIG{'CHLD'}='IGNORE'; use IO::Socket; use FileHandle;"
    $pl_status = "$o=\" [OK]\"; $e=\" Error: \""
    $pl_socket = "socket(SOCKET, PF_INET, SOCK_STREAM,$tcp) or die print\n\"$!$e$!$!\""
    $msg1 = "print \"$! OK! I\\'m successful connected.$!\""
    $msg2 = "print \"$! OK! I\\'m accept connection.$!\""
  condition:
    filesize < 6000 and
    ( $pl_start at 0 and all of ($pl*) ) or
    any of ($msg*)
}
```



## YARA Rules

### Exaramel Backdoor Detection

```
rule APT_MAL_Sandworm_Exaramel_Configuration_Key {  
  meta:  
    author = "FR/ANSSI/SDO"  
    description = "Detects the encryption key for the configuration file used  
by Exaramel malware as seen in sample e1ff72[...]"  
    reference = "https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-  
005.pdf"  
    date = "2021-02-15"  
    score = 80  
  strings:  
    $ = "odhyrfjcnfkdtslt"  
  condition:  
    all of them  
}
```

```
rule APT_MAL_Sandworm_Exaramel_Configuration_Name_Encrypted {  
  meta:  
    author = "FR/ANSSI/SDO"  
    description = "Detects the specific name of the configuration file in  
Exaramel malware as seen in sample e1ff72[...]"  
    reference = "https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-  
005.pdf"  
    date = "2021-02-15"  
    score = 80  
  strings:  
    $ = "configtx.json"  
  condition:  
    all of them  
}
```



## YARA Rules

```
rule APT_MAL_Sandworm_Exaramel_Configuration_File_Plaintext {
  meta:
    author = "FR/ANSSI/SDO"
    description = "Detects contents of the configuration file used by
Exaramel (plaintext)"
    reference = "https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-
005.pdf"
    date = "2021-02-15"
    score = 80
  strings:
    $ = /{"Hosts":\[".{10,512}"\],"Proxy":".{0,512}","Version":".{1,32}","Guid":"/
  condition:
    all of them
}
```

```
rule APT_MAL_Sandworm_Exaramel_Configuration_File_Ciphertext {
  meta:
    author = "FR/ANSSI/SDO"
    description = "Detects contents of the configuration file used by
Exaramel (encrypted with key odhyrfjcnfkdtslt, sample e1ff72[...])"
    reference = "https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-
005.pdf"
    date = "2021-02-15"
    score = 80
  strings:
    $ = { 6F B6 08 E9 A3 0C 8D 5E DD BE D4 } // encrypted with key
odhyrfjcnfkdtslt
  condition:
    all of them
}
```



## YARA Rules

```
rule APT_MAL_Sandworm_Exaramel_Socket_Path {  
    meta:  
        author = "FR/ANSSI/SDO"  
        description = "Detects path of the unix socket created to prevent  
concurrent executions in Exaramel malware"  
        reference = "https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-  
005.pdf"  
        date = "2021-02-15"  
        score = 80  
    strings:  
        $ = "/tmp/.applocktx"  
    condition:  
        all of them }
```

```
rule APT_MAL_Sandworm_Exaramel_Strings_Typo {  
    meta:  
        author = "FR/ANSSI/SDO"  
        description = "Detects misc strings in Exaramel malware with typos"  
        reference = "https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-  
005.pdf"  
        date = "2021-02-15"  
        score = 80  
    strings:  
        $typo1 = "/sbin/init | awk "  
        $typo2 = "Syslog service for monitoring \n"  
        $typo3 = "Error.Can't update app! Not enough update archive."  
        $typo4 = ":\\"metod\""  
    condition:  
        3 of ($typo*) }
```



## YARA Rules

---

```
rule APT_MAL_Sandworm_Exaramel_Task_Names {  
    meta:  
        author = "FR/ANSSI/SDO"  
        description = "Detects names of the tasks received from the CC server in  
Exaramel malware"  
        reference = "https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-  
005.pdf"  
        date = "2021-02-15"  
        score = 80  
    strings:  
        $ = "App.Delete"  
        $ = "App.SetServer"  
        $ = "App.SetProxy"  
        $ = "App.SetTimeout"  
        $ = "App.Update"  
        $ = "IO.ReadFile"  
        $ = "IO.WriteFile"  
        $ = "OS.ShellExecute"  
    condition:  
        all of them  
}
```



## YARA Rules

### Exaramel backdoor detection

```
rule APT_MAL_Sandworm_Exaramel_Struct {
  meta:
    author = "FR/ANSSI/SDO"
    description = "Detects the beginning of type _type struct for some of the
most important structs in Exaramel malware"
    reference = "https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-
005.pdf"
    date = "2021-02-15"
    score = 80
  strings:
    $struct_le_config = {70 00 00 00 00 00 00 00 58 00 00 00 00 00 00 00 47
2d 28 42 0? [2] 19}
    $struct_le_worker = {30 00 00 00 00 00 00 00 30 00 00 00 00 00 00 00
46 6a 13 e2 0? [2] 19}
    $struct_le_client = {20 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 7b
6a 49 84 0? [2] 19}
    $struct_le_report = {30 00 00 00 00 00 00 00 28 00 00 00 00 00 00 00 bf
35 0d f9 0? [2] 19}
    $struct_le_task = {50 00 00 00 00 00 00 00 20 00 00 00 00 00 00 00 88
60 a1 c5 0? [2] 19}
  condition:
    any of them
}
```



## YARA Rules

### Exaramel backdoor detection

```
rule APT_MAL_Sandworm_Exaramel_Strings {  
    meta:  
        author = "FR/ANSSI/SDO (composed from 4 separate rules by Florian Roth)"  
        description = "Detects Strings used by Exaramel malware"  
        reference = "https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-005.pdf"  
        date = "2021-02-15"  
        score = 80  
    strings:  
        $persistence1 = "systemd"  
        $persistence2 = "upstart"  
        $persistence3 = "systemV"  
        $persistence4 = "freebsd rc"  
        $report1 = "systemdupdate.rep"  
        $report2 = "upstartupdate.rep"  
        $report3 = "remove.rep"  
        $url1 = "/tasks.get/"  
        $url2 = "/time.get/"  
        $url3 = "/time.set"  
        $url4 = "/tasks.report"  
        $url5 = "/attachment.get/"  
        $url6 = "/auth/app"  
    condition:  
        ( 5 of ($url*) and all of ($persistence*) ) or  
        ( all of ($persistence*) and all of ($report*) ) or  
        ( 5 of ($url*) and all of ($report*) )  
}
```



## References

---

<https://attack.mitre.org/groups/G0034/>

<https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fattack.mitre.org%2Fgroups%2FG0034%2FG0034-enterprise-layer.json>

<https://apt.etda.or.th/cgi-bin/listgroups.cgi>

<https://www.digitalshadows.com/blog-and-research/mapping-mitre-attck-to-sandworm-aps-global-campaign/>

<https://resources.infosecinstitute.com/topic/apt-sandworm-notpetya-technical-overview/>

<https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and>

<https://malpedia.caad.fkie.fraunhofer.de/actor/sandworm>

[https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report\\_15-06-2021.pdf](https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021.pdf)





## Contact Us

---

Tackling regional and global threat actors requires greater cooperation between the public and private sectors. One of the most significant contributors to this collaboration is the technology partners that provide digital risk protection applications and cyber threat intelligence services. With the services to be received in this area, you can get support on the latest attack trends, vulnerability intelligence, intelligence work for your brand, the technique, tactics, procedures of threat actors, the appearance of your institution on the internet, and attack surface discovery and many more. Brandefense responds to all of these industry needs with an all-in-one perspective, on a single platform, and without the need for any internal installation.

**You can contact us for all your questions and PoC requests;**

**BRANDEFENSE.COM**

+90 (850) 303 85 35

[info@brandefense.com](mailto:info@brandefense.com)



**/Brandefense**



**/brandefense**