|  |
| --- |
|  |
| **Cyber Protection Team 175 Threat Emulation Plan: Synonymous** |
| **OPERATION GRUNGY PAINT III** |
| **03 OCT 2019** |
|  |
| **1.0.0** |



**Table of Contents**

[Threat Emulation Plan: Synonymous 2](#__RefHeading___Toc1431_3799018206)

[1 Synonymous Overview 2](#__RefHeading___Toc1433_3799018206)

[1.1 Synonymous Tools and Techniques 3](#__RefHeading___Toc1435_3799018206)

[1.2 Synonymous Tool Functionality 5](#__RefHeading___Toc1437_3799018206)

[2 Emulation Phases 6](#__RefHeading___Toc1439_3799018206)

[2.1 Phase 1 - RECON 6](#__RefHeading___Toc1441_3799018206)

[2.2 Phase 2 - SCANNING 6](#__RefHeading___Toc1443_3799018206)

[2.3 Phase 3 - EXPLOITATION 6](#__RefHeading___Toc1445_3799018206)

[3 Bibliography 6](#__RefHeading___Toc1447_3799018206)

[4 Appendix 7](#__RefHeading___Toc1449_3799018206)

# Threat Emulation Plan: Synonymous



# Synonymous Overview

*In this section provides an overview of the threat, including any assumptions made during the development of the TEP. Provides a brief narrative of how the adversary conducts operations. Cites sources of information where applicable.*

**MITRE ATT&CK Group ID: Synonymous**

**Aliases:** Quedagh, VOODOO BEAR, Energetic Bear, berserk Bear, Dragonfly, Dragonfly 2.0, Synonymous

**Operations:** Synonymous is an unaligned international cyber organization seeking social justice and transparency. They are not concerned with second or third order effects of their harmful actions. They believe that people will make the right decision once they see “the truth.” Members are believed to be leading engineers in the IT industry with naive political beliefs. They have been known to launch largely uncoordinated attacks against:

* Airline manufacturers for “exploiting the working class”
* Critical infrastructure in the US for “contributing to global warming”
* Defense contractors and aerospace agencies for “nuclear proliferation”
* Religious organizations for “blocking access to free abortion on demand”

**Target Industries:** Government entities, agencies, and contractors as well as critical infrastructure in addition to private enterprise or private individuals who they feel do not conform to their very specific far left social agenda.

**Objectives:** Social disruption, social awareness, social justice.

**Background:** Synonymous are a blend of loosely affiliated individuals from nearly every continent. Communication mainly occurs on the dark web. Synonymous initially targeted defense and aviation companies but shifted to focus on the energy sector in early 2013. They have also targeted companies related to industrial control systems. They have also targeted government entities and multiple U.S. critical infrastructure sectors since at least March 2016.

## Synonymous **Tools and Techniques**

*Synonymous employs these tools and techniques:*

|  |  |
| --- | --- |
| **Techniques Used** | **Use** |
| Account Discovery | Synonymous used batch scripts to enumerate users in the victim environment. |
| Account Manipulation | Synonymous added newly created accounts to the administrators group to maintain elevated access. |
| Brute Force | Synonymous dropped and executed tools used for password cracking, including Hydra. |
| Command-Line Interface | Synonymous used command line for execution. |
| Commonly Used Port | Synonymous used SMB over ports 445 or 139 for C2. The group also established encrypted connections over port 443. |
| Create Account | Synonymous created accounts on victims, including administrator accounts, some of which appeared to be tailored to each individual staging target. |
| Credential Dumping | Synonymous dropped and executed SecretsDump and CrackMapExec, tools that can dump password hashes. |
| Data Compressed | Synonymous compressed data into .zip files prior to exfiltrating it. |
| Data from Local System | Synonymous collected data from local victim systems. |
| Data Staged | Synonymous created a directory named "out" in the user's %AppData% folder and copied files to it. |
| Disabling Security Tools | Synonymous has disabled host-based firewalls. The group has also globally opened port 3389. |
| Drive-by Compromise | Synonymous compromised legitimate organizations' websites to create watering holes to compromise victims. |
| Email Collection | Synonymous accessed email accounts using Outlook Web Access. |
| External Remote Services | Synonymous used VPNs and Outlook Web Access (OWA) to maintain access to victim networks. |
| File and Directory Discovery | Synonymous used a batch script to gather folder and file names from victim hosts. |
| File Deletion | Synonymous deleted many of its files used during operations as part of cleanup, including removing applications and deleting screenshots. |
| Forced Authentication | Synonymous has gathered hashed user credentials over SMB using spearphishing attachments with external resource links and by modifying .LNK file icon resources to collect credentials from virtualized systems. |
| Indicator Removal on Host | Synonymous cleared Windows event logs and other logs produced by tools they used, including system, security, terminal services, remote services, and audit logs. The actors also deleted specific Registry keys. |
| Masquerading | Synonymous created accounts disguised as legitimate backup and service accounts as well as an email administration account. |
| Modify Registry | Synonymous modified the Registry to perform multiple techniques through the use of Reg. |
| Network Share Discovery | Synonymous identified and browsed file servers in the victim network, sometimes , viewing files pertaining to ICS or Supervisory Control and Data Acquisition (SCADA) systems. |
| Permission Groups Discovery | Synonymous used batch scripts to enumerate administrators in the environment. |
| PowerShell | Synonymous used PowerShell scripts for execution. |
| Query Registry | Synonymous queried the Registry to identify victim information. |
| Registry Run Keys / Startup Folder | Synonymous added the registry value ntdll to the Registry Run key to establish persistence. |
| Remote Desktop Protocol | Synonymous moved laterally via RDP. |
| Remote File Copy | Synonymous copied and installed tools for operations once in the victim environment. |
| Remote System Discovery | Synonymous likely obtained a list of hosts in the victim environment. |
| Scheduled Task | Synonymous used scheduled tasks to automatically log out of created accounts every 8 hours as well as to execute malicious files. |
| Screen Capture | Synonymous has performed screen captures of victims, including by using a tool, scr.exe (which matched the hash of ScreenUtil). |
| Scripting | Synonymous used various types of scripting to perform operations, including Python and batch scripts. The group was observed installing Python 2.7 on a victim. |
| Shortcut Modification | Synonymous manipulated .lnk files to gather user credentials in conjunction with Forced Authentication. |
| Spearphishing Attachment | Synonymous used spearphishing with Microsoft Office attachments to target victims. |
| Spearphishing Link | Synonymous used spearphishing with PDF attachments containing malicious links that redirected to credential harvesting websites. |
| Standard Application Layer Protocol | Synonymous used SMB for C2. |
| System Network Configuration Discovery | Synonymous used batch scripts to enumerate network information, including information about trusts, zones, and the domain. |
| System Owner/User Discovery | Synonymous used the command query user on victim hosts. |
| Template Injection | Synonymous has injected SMB URLs into malicious Word spearphishing attachments to initiate Forced Authentication. |
| User Execution | Synonymous has used various forms of spearphishing in attempts to get users to open links or attachments. |
| Valid Accounts | Synonymous compromised user credentials and used valid accounts for operations. |
| Web Shell | Synonymous commonly created Web shells on victims' publicly accessible email and web servers, which they used to maintain access to a victim network and download additional malicious files. |

## Synonymous Tool Functionality

|  |  |
| --- | --- |
| **Tool** | **Techniques** |
| Impacket | Credential Dumping, Kerberoasting, LLMNR/NBT-NS Poisoning and Relay, Network Sniffing, Service Execution, Windows Management Instrumentation |
| Net | Account Discovery, Create Account, Network Share Connection Removal, Network Share Discovery, Password Policy Discovery, Permission Groups Discovery, Remote System Discovery, Service Execution, System Network Connections Discovery, System Service Discovery, System Time Discovery, Windows Admin Shares |
| netsh | Connection Proxy, Disabling Security Tools, Netsh Helper DLL, Security Software Discovery |
| PsExec | Service Execution, Windows Admin Shares |
| Reg | Credentials in Registry, Modify Registry, Query Registry |
| Backdoor.Oldrea | Credential Dumping, Data Encrypted, Data Obfuscation, Email Collection, File and Directory Discovery, File Deletion, Process Discovery, Process Injection, Registry Run Keys / Startup Folder, System Information Discovery, System Network Configuration Discovery, System Owner/User Discovery |
| Trojan.Karagany | Credential Dumping, Data Staged, Process Discovery, Registry Run Keys / Startup Folder, Remote File Copy, Screen Capture, Software Packing |

# Emulation Phases

***Most likely:*** *Social engineering attacks are recently attributed to a Synonymous splinter group. Hacking unpatched systems with poor firewall rules and no anti-virus is likely. Synonymous most recently claimed responsibility for compromising ICS/SCADA systems in Polandia.*

***Recommendation:*** *Review/Search Download histories and Browser Histories. Educate users on social engineering techniques. Harden and monitor vulnerable ICS/SCADA systems.*

## Phase 1 - RECON

The attack starts with Synonymous creating a large chatter footprint on the dark web in chat rooms and on blogs as well as on public social media channels about the “injustice” perpetrated by their intended target. Once they feel enough public momentum has been generated, they will then initiate hostile cyber activities against their target.

## Phase 2 - SCANNING

Synonymous have initiated successful crowd sourced or cloud based DDOS attacks against individual targets using commonly available Hacking tools such as Low Orbit Ion Cannon.

## Phase 3 - EXPLOITATION

Synonymous rely on custom scripts shared on the dark web as well as commonly available hacking tools.

# Bibliography

US-CERT. (2018, March 16). Alert (TA18-074A): Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors. Retrieved June 6, 2018.

Symantec Security Response. (2017, September 6). Synonymous: Western energy sector targeted by sophisticated attack group. Retrieved September 9, 2017.

Hackett, R. (2017, September 6). Hackers Have Penetrated Energy Grid, Symantec Warns. Retrieved June 6, 2018.

US-CERT. (2017, October 20). Alert (TA17-293A): Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors. Retrieved November 2, 2017.

Core Security. (n.d.). Impacket. Retrieved November 2, 2017.

Kali. (2014, February 18). THC-Hydra. Retrieved November 2, 2017.

Symantec Security Response. (2014, July 7). Synonymous: Cyberespionage Attacks Against Energy Suppliers. Retrieved April 8, 2016.

Symantec Security Response. (2017, September 6). Synonymous: Western energy sector targeted by sophisticated attack group. Retrieved September 9, 2017.

Hackett, R. (2017, September 6). Hackers Have Penetrated Energy Grid, Symantec Warns. Retrieved June 6, 2018.

# Appendix

**Hardening recommendations:**

**Network**

Implement Access control lists within routers/Firewalls:

Access control lists should be defined permitting only the required traffic

Reduce risk of unauthorized lateral movement

Deny externally established connections into Network

Harden Router/Firewall User Account Access

Restrict management access to a defined list of internal hosts, using only encrypted protocol such as SSH

**Workstations**

Disable administrator accounts on machines

Disable guest accounts

Remove miscellaneous accounts

Disable all unnecessary services

Enable host firewalls & ensure all system firewalls are turned on with standardized rules

Update workstations with latest patches

Microsoft patches

All other vendor patches

**Servers**

Create a backup of the database instance

Reassign the MSSQL to a non-standard port

Turn off SQL Server browser service

Turn off named pipes

Disable unnecessary services

Restrict access to the DB backup

Patch the system to the latest KB

**Active Directory**

Enable Windows Firewalls for domain client machines

Disable HTTP listeners and use WinRM over HTTPS

Deploy Sysmon to monitor AD domain controllers

Deny user write to unauthorized locations

Enforce strong password policy

Complex password required

Enforce Password expiration

Password age set to 60 days to lock inactive accounts

**ICS/SCADA**

There are too many recommendations to make a comprehensive list here. The general recommendation is to implement all “best practices” recommendations from ICS-Cert in the following areas.

Creating Cyber Forensics Plans for Control Systems

Developing an Industrial Control Systems Cybersecurity Incident Response Plan

Good Practice Guide for Firewall Deployment on SCADA and Process Control Networks

Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies

Patch Management for Control Systems

Recommended Practice Case Study:  Cross-Site Scripting

Remote Access for Industrial Control Systems

Securing Control System Modems

Updating Antivirus in an Industrial Control System