



Cerulean Shield Cyber Incident Report

Date: 9/14/2023

Name of individual
completing this form:

Tracking
number: CS23-00001

Incident Priority

<input checked="" type="checkbox"/> HIGH	<input type="checkbox"/> MEDIUM	<input type="checkbox"/> LOW	<input type="checkbox"/> OTHER
<i>Additional notes:</i>			

Incident Type

Check all that apply.

<input checked="" type="checkbox"/> Compromised System <input checked="" type="checkbox"/> Compromised User Credentials (e.g., lost password) <input checked="" type="checkbox"/> Network Attack (e.g., DoS) <input checked="" type="checkbox"/> Malware (e.g., virus, worm, Trojan) <input checked="" type="checkbox"/> Reconnaissance (e.g., scanning, sniffing)	<input type="checkbox"/> Lost Equipment/Theft <input type="checkbox"/> Physical Break-in <input type="checkbox"/> Social Engineering (e.g., Phishing) <input type="checkbox"/> Law Enforcement Request <input type="checkbox"/> Policy Violation (e.g., acceptable use) <input type="checkbox"/> Unknown/Other (Please describe below.)
<i>Incident description notes:</i> Threat Actors accessed the SimCorp AWS VPC using stolen corporate VPN credentials and conducted active reconnaissance using port scanning techniques. Threat actors attempted brute force login attacks on all instances, successfully gained access to some, installed malware/trojans, and likely exfiltrated data. The attack rendered one system non-operational.	

Incident Timeline

Please provide as much detail as possible.

<input type="checkbox"/> Date and time when the incident was discovered	Monday, September 11 2023 @ 1000 (PST)
<input type="checkbox"/> Date and time when the incident was reported	09-11-2023 13:18:20
<input type="checkbox"/> Date and time when the incident occurred	09-11-2023 13:18:20

Additional timeline details: The Metasploitable instance was attacked in a 2-hour window starting at 1000 11 SEP 2023 while the instance used a public IP address to download security tools from the internet. Evidence suggests that the metasploitable instance was targeted by the Purple Fox criminal threat group from India.

A separate group of Threat Actors accessed the SimCorp AWS VPC using stolen corporate VPN credentials starting at 12:00 PM PST, 11 SEP . The threat actors attacked the metasploitable3, Accounting1, Web1, and Risk Analyst1 instances with various TTPs. At 12:00 13 SEP, threat actors expanded their attack to include the CFO-Laptop, Accounting2, and Data Analytics Server instances.

Incident Scope

Please provide as much detail as possible.

<input type="checkbox"/> Estimated quantity of systems affected	1 system rendered non-operational (Metasploitable EC2 instance). 4 systems with IOCs: <ul style="list-style-type: none"> - Accounting1 and Accounting2 - successful spoofed logons and creation of new accounts. Accounting1 had potential for remote execution through mimikatz. - Web1 - successful injection attack resulting in exposed data and credential hashes. - Risk-Analyst1 - successful spoofed logins and new accounts creations -
<input type="checkbox"/> Estimated quantity of users affected	~ 12 Users
<input type="checkbox"/> Third parties involved or affected (e.g., vendors, contractors, partners)	SimpCorps financial services clients

Additional scoping information:

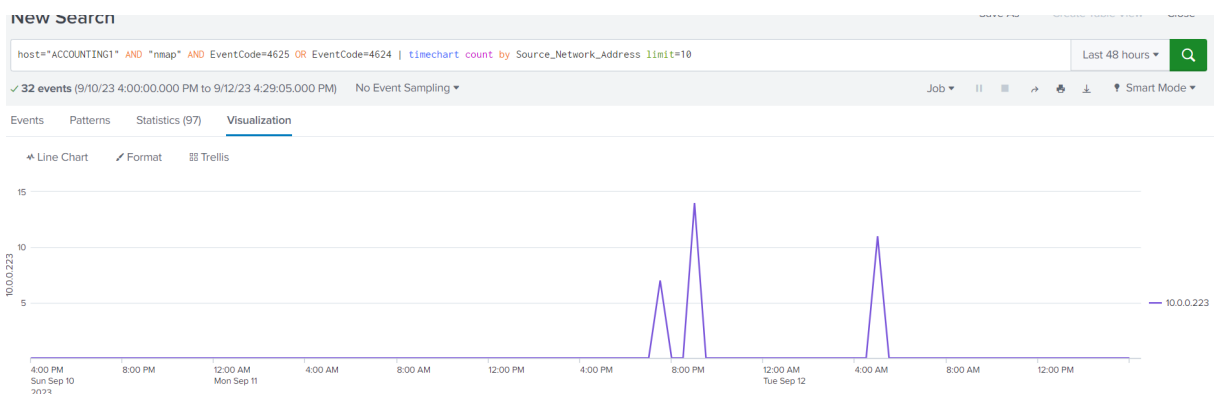
MITRE TTPs for Purple Fox:

T1059 - Command and Scripting Interpreter
T1068 - Exploitation of Privilege Escalation
T1014 - Rootkit
T1027- Obfuscated Files or Information
T1112 - Modify Registry
T1543.003 - Create or Modify System Process: Windows Service
T1071.001 - Application Layer Protocol: Web Protocols

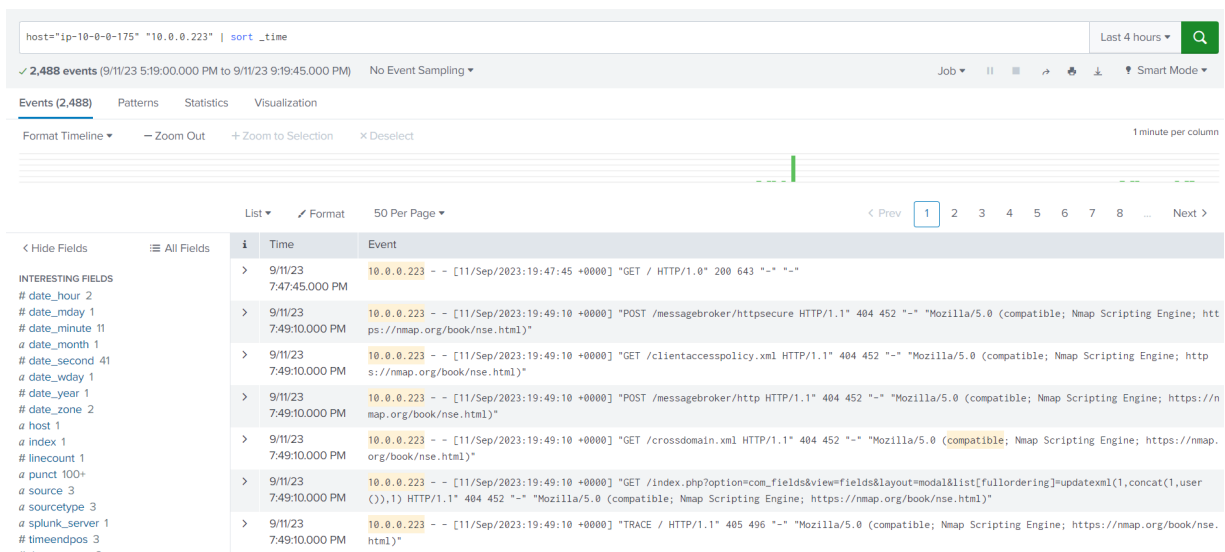
MITRE TTPs for Red Team Threat Actors:

Reconnaissance:

T1595 Active Scanning



T1593 Search Open Websites/Domains



Resource Development:

T1650 Acquire Access
T1586 Compromise Accounts
T1584 Compromise Infrastructure
T1588 Obtain Capabilities

Threats found. Start the recommended actions.

HackTool:Win32/LSADump!dha

Alert level: High

Status: Active

Date: 9/13/2023 12:58 PM

Category: Tool

Details: This program has potentially unwanted behavior.

[Learn more](#)

Affected items:

file: C:\Users\accounting\Desktop\Tools\mimikatz-executable
\Win32\mimikatz.exe

file: C:\Users\general-user\Desktop\Tools\mimikatz-executable
\Win32\mimikatz.exe

OK

sers > accounting > Desktop > Tools > mimikatz-executable > Win32

mimikatz.exe Properties

Security


General

Details

Compatibility

Previous Versions

Digital Signatures



mimikatz.exe

Type of file:

Application (.exe)

Description:

mimikatz for Windows

Location:

C:\Users\accounting\Desktop\Tools\mimikatz-executable

Size:

1.01 MB (1,064,944 bytes)

Size on disk:

1.01 MB (1,064,960 bytes)

Created:

Monday, June 7, 2021, 6:49:29 AM

Modified:

Monday, June 7, 2021, 6:45:50 AM

Accessed:

Monday, June 7, 2021, 6:49:29 AM

Attributes:

☐ Read-only

☐ Hidden

Advanced...

Security:

This file came from another computer and might be blocked to help protect this computer.

☐ Unblock

OK

Cancel

Apply

Initial Access:
T1190 Exploit Public-Facing Application



Add someone else to this PC



accounting
Local account



admin1
Administrator - Local account

Change account type

Remove



general-user
Local account



user
Local account

T1078 Valid Accounts

host="ACCOUNTING1" EventCode=4720

✓ 1 event (9/7/23 2:00:00.000 PM to 9/14/23 2:08:59.000 PM) No Event Sampling

Events (1) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect

List Format 50 Per Page

	i	Time	Event
INTERESTING FIELDS	9/13/23	09/13/2023 04:33:18 PM	
# EventCode 1	11:33:18.000 PM		LogName=Security
α host 1			EventCode=4720
α index 1			EventType=0
# linecount 1			ComputerName=accounting1
α Message 1			Show all 49 lines
α source 1			
α sourcetype 1			
α splunk_server 1			

+ Extract New Fields

Event Actions

Type	Field	Value
Event	EventCode	4720
	Message	A user account was created. Subject: Security ID: S-1-5-21-2020954294-3820947412-549806118-500 Account Name: Administrator Account Domain: ACCOUNTING1 Logon ID: 0x19D50EC New Account: Security ID: S-1-5-21-2020954294-3820947412-549806118-1005 Account Name: admin1 Account Domain: ACCOUNTING1 Attributes: SAM Account Name: admin1 Display Name: <value not set> User Principal Name: - Home Directory: <value not set> Home Drive: <value not set> Script Path: <value not set> Profile Path: <value not set> User Workstations: <value not set> Password Last Set: <never> Account Expires: <never> Primary Group ID: 513 Allowed To Delegate To: - Old UAC Value: 0x0 New UAC Value: 0x15 User Account Control: Account Disabled 'Password Not Required' - Enabled 'Normal Account' - Enabled User Parameters: <value not set> SID History: - Logon Hours: All Additional Information: -

Privilege Escalation:

T1548 Abuse Elevation Control Mechanism

✓	9/13/23 11:35:40.000 PM	09/13/2023 04:35:40 PM LogName=Security EventCode=4732 EventType=0 ComputerName=accounting1 SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=434480 Keywords=Audit Success TaskCategory=Security Group Management OpCode=Info Message=A member was added to a security-enabled local group. Subject: Security ID: S-1-5-21-2020954294-3820947412-549806118-500 Account Name: Administrator Account Domain: ACCOUNTING1 Logon ID: 0x19D50EC Member: Security ID: S-1-5-21-2020954294-3820947412-549806118-1005 Account Name: - Group: Security ID: S-1-5-32-544 Group Name: Administrators Group Domain: Builtin Additional Information: Privileges: -
---	----------------------------	---

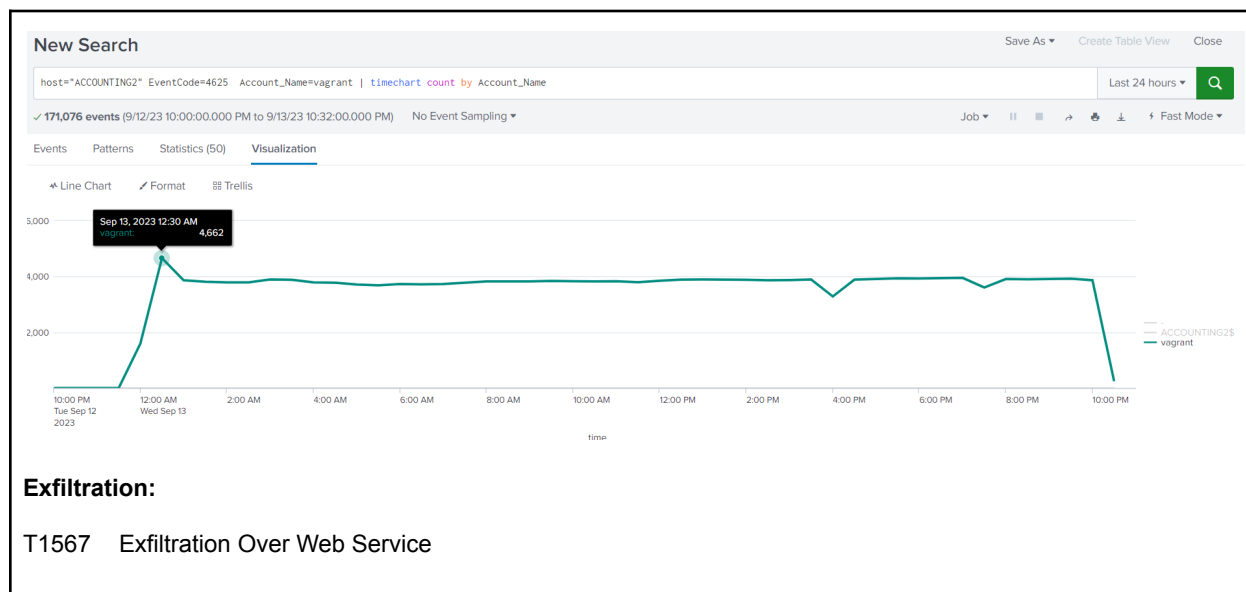
T1021 Remote Services

IP address ▾	Local port ▾	Remote port ▾	Inbound traffic ▾	Outbound traffic ▾	Protocol
10.0.0.223	21	-	17.2 kB	20.9 kB	TCP
10.0.0.223	3389	-	71.6 MB	53.8 MB	TCP
10.0.0.223	443	-	88 B	80 B	TCP
103.149.92.238	-	15255	0 B	624 B	TCP
103.39.232.44	-	11499	0 B	624 B	TCP
103.44.239.201	-	12924	0 B	832 B	TCP
103.55.60.10	-	10492	0 B	208 B	TCP
112.49.122.85	-	10942	0 B	624 B	TCP
114.244.48.11	-	11471	0 B	208 B	TCP
120.25.76.236	-	15123	0 B	208 B	TCP

9/13/23
9:34:07000 PM

89/13/2023 02:34:07 PM
LogName=Security
EventCode=4625
EventType=0
ComputerName=accounting2
Show all 61 lines
Event Actions ▾

Type	Field	Value	Actions	
Event	Account_Domain ▾	-	▾	
	Account_Name ▾	-	▾	
		vagrant	▾	
	Authentication_Package ▾	NTLM	▾	
	Caller_Process_ID ▾	0x0	▾	
	Caller_Process_Name ▾	-	▾	
	ComputerName ▾	accounting2	▾	
	EventCode ▾	4625	▾	
	EventType ▾	0	▾	
	Failure_Reason ▾	Unknown user name or bad password.	▾	
	Key_Length ▾	0	▾	
	Keywords ▾	Audit Failure	▾	
	LogName ▾	Security	▾	
	Logon_ID ▾	0x0	▾	
	Logon_Process ▾	NtLmSsp	▾	
	Logon_Type ▾	3	▾	
	Message ▾	An account failed to log on. Subject: Security ID: S-1-0-0 Account Name: - Account Domain: - Logon ID: 0x0 Logon Type: 3 Account For Which Logon Failed: Security ID: S-1-0-0 Account Name: vagrant Account Domain: Failure Information: Failure Reason: Unknown user name or bad password. Status: 0xC000006D Sub Status: 0xC0000064 Process Information: Caller Process ID: 0x0 Caller Process Name: - Network Information: Workstation Name: kall Source Network Address: 10.0.0.176 Source Port: 0 Detailed Authentication Information: Logon Process: NtLmSsp Authentication Package: NTLM Transited Services: - Package Name (NTLM only): - Key Length: 0 This event is generated when a logon request fails. It is generated on the computer where access was attempted. The Subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe. The Logon Type field indicates the kind of logon that was requested. The most common types are 2 (interactive) and 3 (network). The Process Information fields indicate which account and process on the system requested the logon. The Network Information fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases. The authentication information fields provide detailed information about this specific logon request. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.		▾



Systems Affected by the Incident

Please provide as much detail as possible.

<input type="checkbox"/> Attack sources (e.g., IP address, port)	IP: 64.227.152.193 Location: Bengaluru, India Port: 18336 Open VPN Access Servers IP: 10.0.0.176, 10.0.0.223 Port: 58706
<input type="checkbox"/> Attack destinations (e.g., IP address, port)	Public IP: 52.40.120.244 Private IP: 10.0.0.82 Port: 58706
<input type="checkbox"/> IP addresses of the affected systems	Metasploitable - Public: 52.40.120.244/Private: 10.0.0.82 Accounting1 - 10.0.0.126 Accounting2 - 10.0.0.197 Web1 - 10.0.0.175 CFO-Laptop - 10.0.0.206 Data Analytics Server - 10.0.0.123 RiskAnalyst1 - 10.0.0.74
<input type="checkbox"/> Primary functions of the affected systems (e.g., web server, domain controller)	Metasploitable - Domain Controller Accounting1 - Accounting Server Accounting2 - Accounting Server Web1 - Web Server CFO-Laptop - Personal Workstation Data Analytics Server - Data processing/storage RiskAnalyst1 - Workstation for data processing

Additional user details:

Incident Handling Log

Please provide as much detail as possible.

<input type="checkbox"/> Actions taken to identify the affected resources	GuardDuty alerts notified us of communication with a known C2 server and specified metasploitable as the affected resource
<input type="checkbox"/> Actions taken to remediate the incident	Elastic IP was removed from instance to stop public access
<input type="checkbox"/> Actions planned to prevent similar incidents	Fix vulnerabilities exploited to access the metasploitable instance, upgrade server to OS version supported by Microsoft (2019)
<i>Additional remediation details: Implement regular security patching in an isolated environment to reduce the chance of lateral movement by threat actors.</i>	

Incident Reporting Information

Complete this section if incident report was system generated.

<input type="checkbox"/> Software package	n/a
<input type="checkbox"/> Host ID and location	n/a

Additional system information:

Complete this section if an incident report was submitted by an individual.

<input type="checkbox"/> Full name	Benjamin Hobbs
<input type="checkbox"/> Job title	SOC Analyst Tier I
<input type="checkbox"/> Business unit	Western Regional Headquarters Unit, North America, SimCorp
<input type="checkbox"/> Work phone	894-130-7493
<input type="checkbox"/> Mobile phone	304-797-6970
<input type="checkbox"/> Email address	bhobbs@nasimcorp.com

Additional contact information:

Incident Contact Information

<input type="checkbox"/> Full name	Chris Bennett
<input type="checkbox"/> Job title	SOC Analyst Tier I

<input type="checkbox"/> Business unit	Western Regional Headquarters Unit, North America, SimCorp
<input type="checkbox"/> Work phone	894-130-3468
<input type="checkbox"/> Mobile phone	304-797-4562
<input type="checkbox"/> Physical location of affected systems (e.g., state, city, building, room, desk)	cbennett@nasimcorp.com

<input type="checkbox"/> Full name	Robert Gillespie
<input type="checkbox"/> Job title	SOC Analyst Tier II
<input type="checkbox"/> Business unit	Western Regional Headquarters Unit, North America, SimCorp
<input type="checkbox"/> Work phone	894-130-5556
<input type="checkbox"/> Mobile phone	304-797-2734
<input type="checkbox"/> Physical location of affected systems (e.g., state, city, building, room, desk)	rgillespie@nasimcorp.com

<input type="checkbox"/> Full name	Gerald Reitmeyer
<input type="checkbox"/> Job title	SOC Analyst Tier II
<input type="checkbox"/> Business unit	Western Regional Headquarters Unit, North America, SimCorp
<input type="checkbox"/> Work phone	894-154-7985
<input type="checkbox"/> Mobile phone	304-686-3052
<input type="checkbox"/> Physical location of affected systems (e.g., state, city, building, room, desk)	greitmeyer@nasimcorp.com

<input type="checkbox"/> Full name	Jonathan McMullin
<input type="checkbox"/> Job title	Senior SOC Analyst Tier III
<input type="checkbox"/> Business unit	Western Regional Headquarters Unit, North America, SimCorp
<input type="checkbox"/> Work phone	894-130-3952

<input type="checkbox"/> Mobile phone	304-797-1043
<input type="checkbox"/> Physical location of affected systems (e.g., state, city, building, room, desk)	jmcmullin@nasimcorp.com

<input type="checkbox"/> Full name	Marco Vazquez
<input type="checkbox"/> Job title	SOC Manager
<input type="checkbox"/> Business unit	Western Regional Headquarters Unit, North America, SimCorp
<input type="checkbox"/> Work phone	894-187-0126
<input type="checkbox"/> Mobile phone	164-832-2017
<input type="checkbox"/> Physical location of affected systems (e.g., state, city, building, room, desk)	mvazquez@nasimcorp.com

<input type="checkbox"/> Full name	Brook Riggio
<input type="checkbox"/> Job title	CISO
<input type="checkbox"/> Business unit	Western Regional Headquarters Unit, North America, SimCorp
<input type="checkbox"/> Work phone	894-130-5556
<input type="checkbox"/> Mobile phone	304-797-2734
<input type="checkbox"/> Physical location of affected systems (e.g., state, city, building, room, desk)	rgillespie@nasimcorp.com

<input type="checkbox"/> Full name	Georg Hetrodt
<input type="checkbox"/> Job title	Chief Operating Officer
<input type="checkbox"/> Business unit	SimCorp
<input type="checkbox"/> Work phone	546-678-4956
<input type="checkbox"/> Mobile phone	283-456-9486
<input type="checkbox"/> Physical location of affected	None

systems (e.g., state, city, building, room, desk)	
---	--

<input type="checkbox"/> Full name	Christian Kromann
<input type="checkbox"/> Job title	Chief Executive Officer
<input type="checkbox"/> Business unit	SimCorp
<input type="checkbox"/> Work phone	650-349-5986
<input type="checkbox"/> Mobile phone	650-385-5732
<input type="checkbox"/> Physical location of affected systems (e.g., state, city, building, room, desk)	None