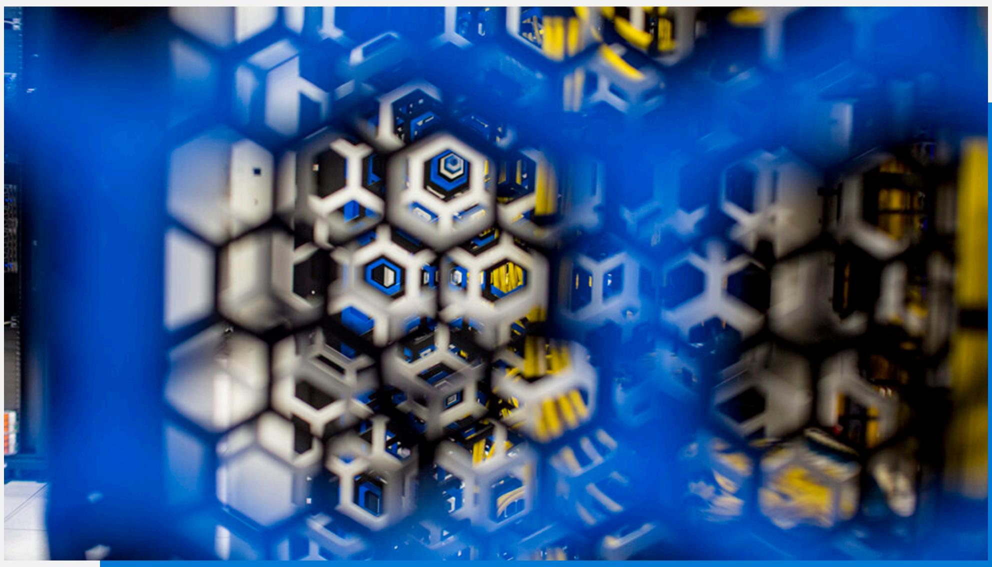


Research Threat intelligence Microsoft Defender Attacker techniques, tools, and infrastructure

19 min read

ACTINIUM targets Ukrainian organizations

By Microsoft Digital Security Unit (DSU)
Microsoft Threat Intelligence

February 4, 2022

Microsoft Defender for Endpoint

Microsoft Defender for Office 365

Attacker techniques, tools, and infrastructure

more

April 2023 update – Microsoft Threat Intelligence has shifted to a new threat actor naming taxonomy aligned around the theme of weather. **ACTINIUM** is now tracked as **Aqua Blizzard** and **DEV-0586** is now tracked as **Cadet Blizzard**.

To learn about how the new taxonomy represents the origin, unique traits, and impact of threat actors, and to get a complete mapping of threat actor names, read this blog: **Microsoft shifts to a new threat actor naming taxonomy**.

The Microsoft Threat Intelligence Center (MSTIC) is sharing information on a threat group named ACTINIUM, which has been operational for almost a decade and has consistently pursued access to organizations in Ukraine or entities related to Ukrainian affairs. MSTIC previously tracked ACTINIUM activity as DEV-0157, and this group is also referred to publicly as Gamaredon.

NOTE: *This blog is available in Ukrainian on the Microsoft CEE Multi-Country News Center to help organizations in Ukraine implement protections against this activity: АКТИНІЙ(ACTINIUM) атакує українські організації.*

In the last six months, MSTIC has observed ACTINIUM targeting organizations in Ukraine spanning government, military, non-government organizations (NGO), judiciary, law enforcement, and non-profit, with the primary intent of exfiltrating sensitive information, maintaining access, and using acquired access to move laterally into related organizations. MSTIC has observed ACTINIUM operating out of Crimea with objectives consistent with cyber espionage. The Ukrainian government has publicly attributed this group to the Russian Federal Security Service (FSB).

Since October 2021, ACTINIUM has targeted or compromised accounts at organizations critical to emergency response and ensuring the security of Ukrainian territory, as well as organizations that would be involved in coordinating the distribution of international and humanitarian aid to Ukraine in a crisis. As with any observed nation-state actor activity, Microsoft directly notifies customers of online services that have been targeted or compromised, providing them with the information they need to secure their accounts. Microsoft has shared this information with Ukrainian authorities.

ACTINIUM represents a unique set of activities separate from the destructive malware attacks by DEV-0586 described in an earlier blog post. As of this writing, MSTIC has not found any indicators correlating these two actors or their operations. The observed ACTINIUM activities detailed in this blog have been limited only to organizations within Ukraine. We have not seen this actor using any unpatched vulnerabilities in Microsoft products or services.

Given the geopolitical situation and the scale of observed activity, MSTIC is prioritizing sharing our knowledge of ACTINIUM tactics, techniques, and procedures (TTPs), along with a significant number of indicators of compromise (IOCs) from our extensive analysis. Our goal is to give organizations the latest intelligence to guide investigations into potential attacks and information to implement proactive protections against future attempts.

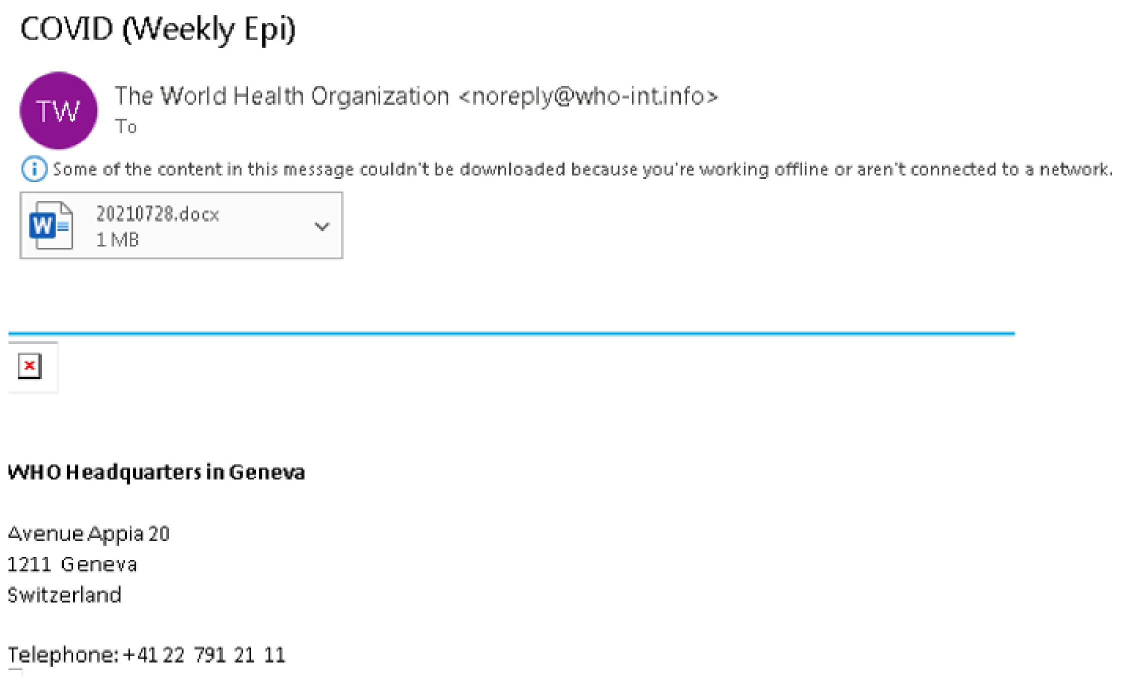
Activity description

Microsoft has observed a repeated set of techniques and procedures throughout operations by ACTINIUM, with several significant elements that we believe are important to understanding these activities. It's important to note that ACTINIUM's tactics are constantly evolving; the activities described in this blog are some of the most consistent and notable observations by Microsoft, but these are not all-encompassing of actor TTPs.

Phishing using remote templates

One of the access vectors most used by ACTINIUM is spear-phishing emails with malicious macro attachments that employ remote templates. Remote template injection refers to the method of causing a document to load a remote document template that contains the malicious code, in this case, macros. Delivery using remote template injection ensures that malicious content is only loaded when required (for example, when the user opens the document). This helps attackers to evade static detections, for example, by systems that scan attachments for malicious content. Having the malicious macro hosted remotely also allows an attacker to control when and how the malicious component is delivered, further evading detection by preventing automated systems from obtaining and analyzing the malicious component.

MSTIC has observed a range of email phishing lures used by ACTINIUM, including those that impersonate and masquerade as legitimate organizations, using benign attachments to establish trust and familiarity with the target.



COVID (Weekly Epi)

The World Health Organization <noreply@who-int.info>
To

Some of the content in this message couldn't be downloaded because you're working offline or aren't connected to a network.

20210728.docx
1 MB

WHO Headquarters in Geneva

Avenue Appia 20
1211 Geneva
Switzerland

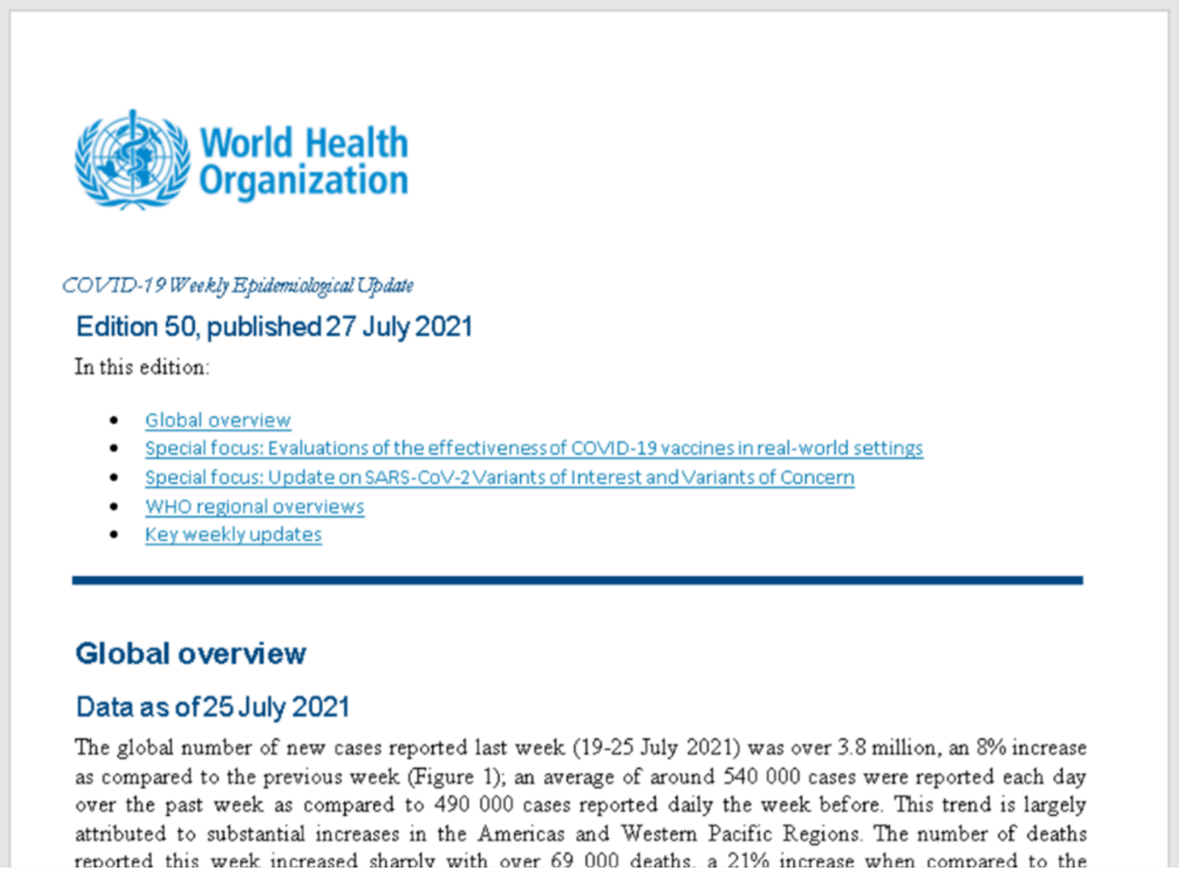
Telephone: +41 22 791 21 11

This phishing email from ACTINIUM uses the sender domain who-int[.]info to masquerade as the legitimate who.int domain, assessed to be impersonating the World Health Organization

Within the body of phishing messages, ACTINIUM has been observed to insert web bugs, which are small external image references that enable the actor to track when a message has been opened and rendered. These web bugs are not malicious by themselves but may indicate that the email is intended for malicious use. Here's an example of a web bug used by ACTINIUM:

```
<img src="http://eyeofra[.]ru/images/icons/312rz45d7/43oFI4b/cached.gif"
height="0" width="10" style="height:0px;width:10pxpx">
```

ACTINIUM's lure documents appear to be legitimate and vary in style and content. For example, the lure document below included a remote template at the following URL: hxxp://usa-national[.]info/USA/sensible[.]dot. While a domain was used in this instance, links with static IP addresses have also been used.



World Health Organization

COVID-19 Weekly Epidemiological Update

Edition 50, published 27 July 2021

In this edition:

- Global overview
- Special focus: Evaluations of the effectiveness of COVID-19 vaccines in real-world settings
- Special focus: Update on SARS-CoV-2 Variants of Interest and Variants of Concern
- WHO regional overviews
- Key weekly updates

Global overview

Data as of 25 July 2021

The global number of new cases reported last week (19-25 July 2021) was over 3.8 million, an 8% increase as compared to the previous week (Figure 1); an average of around 540 000 cases were reported each day over the past week as compared to 490 000 cases reported daily the week before. This trend is largely attributed to substantial increases in the Americas and Western Pacific Regions. The number of deaths reported this week increased sharply with over 69 000 deaths, a 21% increase when compared to the

This URL and the related lure .dot document from ACTINIUM is responsible for loading the malicious remote template. This document uses text from a legitimate who.int situational COVID-19 update report published on July 27, 2021.

ACTINIUM phishing attachments contain a first-stage payload that downloads and executes further payloads. There may be multiple subsequent "staging" scripts before a more fully-featured malicious capability is deployed to a compromised device. It's unclear why there are often multiple stages; one hypothesis is that these staging VBScripts are easier to modify to incorporate new obfuscation or command-and-control (C2) changes. It's also possible that ACTINIUM deploys these scripts to provide some assurance that detection systems are less likely to detect their main capabilities. These initial staging capabilities vary; examples include heavily obfuscated VBScripts, obfuscated PowerShell commands, self-extracting archives, LNK files, or a combination of these. ACTINIUM frequently relies on scheduled tasks in these scripts to maintain persistence. More information on some of the capabilities analyzed by MSTIC is included in the "Malware and capabilities" section.

ACTINIUM operational infrastructure and wordlists

MSTIC assesses that ACTINIUM maintains a large quantity and degree of variation of its operational infrastructure to evade detection. ACTINIUM's operational infrastructure consists of many domains and hosts to facilitate payload staging and C2. In a single 30-day snapshot, MSTIC saw ACTINIUM utilizing over 25 new unique domains and over 80 unique IP addresses, demonstrating that they frequently modify or alter their infrastructure.

ACTINIUM domain name DNS records frequently change, perhaps not frequently enough to be considered "fast-flux", but most DNS records for the domains change once a day on average. More than 70% of the recent 200+ ACTINIUM IP addresses are owned by ASN 197695 – REG.RU. Most ACTINIUM domains are also registered through the same owning company registrar (REG.RU). It is unclear why ACTINIUM appears to favor these legitimate providers.

Malware authored by ACTINIUM often utilizes randomized subdomains for C2. These subdomains have included the use of an apparent English wordlist in their generation procedure, making the domains appear more legitimate while frustrating network defense tools that may rely on domain name blocks. A list of the most common words MSTIC has observed is included in the IOCs below. Within the last 30 days, MSTIC has observed randomized schemes being used increasingly for subdomain patterns instead of wordlists, indicating a possible shift in methodology. One example of this randomization is the effect of their PowerShell stager using the *Get-Random* cmdlet:’

Examples of ACTINIUM subdomains encompassing both wordlists and randomized subdomains include:

- Jealousy[.]Jonas[.]artisola[.]ru
- Deliberate[.]brontaga[.]ru
- registration83[.]alteration[.]luck[.]mirotas[.]ru
- 001912184[.]retarus[.]ru
- 637753599292688334[.]jolotras[.]ru

While the fast-flux nature of ACTINIUM infrastructure means that IP addresses are less useful IOCs, there is a clear preference for it on a specific ASN. Such preference may help defenders determine whether a domain may be more likely to be owned by ACTINIUM. A list of more recent IP addresses is included in the IOCs below.

ACTINIUM appears to employ this same wordlist to obfuscate other aspects of their attacks. For example, as previously mentioned, ACTINIUM often maintains persistence by using scheduled tasks to run their malicious payloads. The payloads are often named with seemingly random words and phrases with valid (but irrelevant) extensions. The files are then executed using scripts with the */E:VBScript* flag to specify the VBScript engine (and to effectively ignore the random file extension assigned to the payload) and the */b* flag to mute alerts and errors. The following is an example:

The terms *deep-grounde*d, *deerfield*, and *defiance* above are used as the name of a scheduled task, a folder name, and a file name, respectively. Terms generated from the wordlist, like those in the example above, have been generated and used on multiple targets and are also used to generate subdomains as previously described. These generated terms may frustrate network defenders as the names of scheduled tasks, file names, and others are almost never the same for each target. We have compiled a list of the terms that MSTIC has observed in the IOCs provided below. Network defenders may be able to use the said list to determine whether a scheduled task, file, or domain is likely to warrant further investigation.

Maintaining persistence and gathering intelligence

MSTIC assesses that the primary outcome of activities by ACTINIUM is persistent access to networks of perceived value for the purpose of intelligence collection. Despite seemingly wide deployment of malicious capabilities in the region, follow-on activities by the group occur in areas of discrete interest, indicating a possible review of targeting. Following initial access, MSTIC has observed ACTINIUM deploying tools such as “Pterodo” to gain interactive access to target networks. In some cases, MSTIC has observed deployments of UltraVNC to enable a more interactive connection to a target. UltraVNC is a legitimate and fully-featured open-source remote desktop application that allows ACTINIUM to easily interact with a target host without relying on custom, malicious binaries that may be detected and removed by security products.

Malware and capabilities

ACTINIUM employs a variety of malware families with assessed objectives to deploy remotely retrieved or embedded payloads before execution. MSTIC has analyzed several of these payloads and tracks the rapidly developing binaries as the following families: DinoTrain, DesertDown, DilongTrash, ObfuBerry, ObfuMerry, and PowerPunch. The PowerPunch malware family is an excellent example of an agile and evolving sequence of malicious code and is further explained below.

The actor quickly develops new obfuscated and lightweight capabilities to deploy more advanced malware later. These are fast-moving targets with a high degree of variance. Analyzed payloads regularly place a strong emphasis on obfuscated VBScripts. As an attack, this is not a novel approach, yet it continues to prove successful as antivirus solutions must consistently adapt to keep pace with a very agile threat.

The most feature-rich malware family we track relating to ACTINIUM activity is known widely within the industry as “Pterodo”. In the following sections, we break down Pterodo further and review a binary called QuietSieve that is specifically geared toward file exfiltration and monitoring.

PowerPunch

The droppers and downloader family names tend to be fast-moving targets due to the heavy use of obfuscation and simple functionality. For example, PowerPunch is executed from within PowerShell as a one-line command, encoded using Base64:

These binaries also exhibit features that rely on data from the compromised host to inform encryption of the next stage. PowerPunch also provides an excellent example of this. In the following code snippet, the VolumeSerialNumber of the host serves as the basis for a multibyte XOR key. The key is applied to an executable payload downloaded directly from adversary infrastructure, allowing for an encryption key unique to the target host (highlighted variables names were changed for clarity).

Ultimately, a next-stage executable is remotely retrieved and dropped to disk prior to execution.

Pterodo

MSTIC has also reviewed several variants of ACTINIUM's more fully-featured Pterodo malware. A couple of features play a direct role in this malware's ability to evade detection and thwart analysis: its use of a dynamic Windows function hashing algorithm to map necessary API components, and an "on-demand" scheme for decrypting needed data and freeing allocated heap space when used.

The function hashing algorithm is used to map a hash value of a given function name to its corresponding location in memory using a process known as Run-Time Dynamic Linking. Pre-computed hashes are passed to the hashing algorithm alongside the Windows library containing the related function name. Each function name within the library is hashed; when a match is found, its address is saved.

The hashing algorithm itself has historically not been terribly complex, and when considering an example such as SHA-256 51b9e03db53b2d583f66e47af56bb0146630f8a175d4a439369045038d6d2a45, it may be emulated using Python logic as follows:

When pre-computing these hashes over different Windows DLLs commonly used in schemes like this, it is possible to map out these hash values and the corresponding Windows function name using open-source tools like the MITRE malchive.

We have seen this behavior in many different malware families before. The hashing algorithm has been consistent within those families, allowing analysis like this to scale forward. Unfortunately, in Pterodo's case, there is far too much drift in the algorithm for it to be used reliably. The algorithm has been different in many of the samples we've reviewed. Additionally, the application of this technique seems to vary among samples. Some samples have been observed to use it for most Windows function calls, while others have used it very sparingly.

However, Windows libraries need to be loaded before function hashes are computed. The names of these libraries and other strings required by the malware are recovered using an "on-demand" scheme that decrypts the data, uses it, and immediately frees the associated heap space once it is no longer needed.

As seen in the screenshot above, data is passed into a decryption function before being used in a call to *GetModuleHandleA*. Before the hashing routine uses the module handle, the decrypted string representing the function name has its associated heap space freed and may be later overwritten. However, the reconstruction of this data is straightforward within the two core decryption algorithms we have observed. The first one relies on an encrypted blob whose first value is interpreted as the size of the decrypted data in DWORD (four-byte) chunks.

This data is decrypted four bytes at a time, with the last byte being the encrypted content. Each encrypted byte is XOR'd using a multibyte key sequence unique to each sample reviewed. In our example, the ASCII key sequence *39d84sdfjh* is applied to the content above to produce the module name *Kernel32*.

A slight deviation from this approach was also uncovered in samples such as SHA-256 2042a2feb4d9f54d65d7579a0afba9ee1c6d22e29127991fbf34ea3da1659904, where the decryption algorithm is passed data representing two WORD values: one mapping to the offset of the encrypted content within the malware and another representing the length. These parameters are recovered, and a much longer multibyte XOR sequence is applied to the encrypted content after the starting index is computed.

Application of either approach allows us to gain a greater level of analysis into strings used by the malware. Continuing with the approach used by the previously cited example, we can apply the multibyte XOR key over the entire encrypted data space, resulting in the following content:

Pterodo has been observed to be a constantly evolving malware family with a range of capabilities intended to make analysis more difficult. By applying our understanding, we can expose more malware elements to further advance mitigation and detection efforts.

QuietSieve

The QuietSieve malware family refers to a series of heavily-obfuscated .NET binaries specifically designed to steal information from the target host. Before enumerating target files on the host, QuietSieve first checks for connectivity by sending a test ping to 8.8.8.8 (Google public DNS). The creation of the buffer for the ICMP request is done manually within QuietSieve and contains all null values for the 32-byte data portion of the ICMP packet. If this check succeeds, a randomly-generated alphanumeric prefix is created and combined with the callback domain as a subdomain before an initial request is made over HTTPS.

If the connection is successful, the following file name extensions are searched for within removable, fixed, or networked drives: *doc*, *docx*, *xls*, *rtf*, *odt*, *txt*, *jpg*, *pdf*, *rar*, *zip*, and *7z*. Candidate files are queued up for upload. They are also inventoried via a specific MD5 hash value computed based on attributes of the target file and compromised host, such as the volume serial number, file size, and last write timestamp assigned to the file. Computed hashes are logged to an inventory log file that serves as a reference point checked by the malware to avoid duplicate exfiltration. QuietSieve will also take screenshots of the compromised host approximately every five minutes and save them in the user's local *Application Data* folder under *Temp\SymbolSourceSymbols\icons* or *Temp\ModeAuto\icons* using the format *yyyy-MM-dd-HH-mm* along with the *jpg* file extension.

While the QuietSieve malware family is primarily geared towards the exfiltration of data from the compromised host, it can also receive and execute a remote payload from the operator. These payloads are written to the user's *Application Data* folder with a random alphanumeric name and are executed in a hidden window.

Microsoft will continue to monitor ACTINIUM activity and implement protections for our customers.

Indicators of compromise (IOCs)

The following IOCs were observed during our investigation. We encourage our customers to investigate these indicators in their environments and implement detections and protections to identify past related activity and prevent future attacks against their systems.

Analyst note on ACTINIUM IOCs: ACTINIUM registers and administers a large amount of infrastructure. It's not always possible to accurately determine what malicious component connects to which C2 infrastructure. MSTIC has observed cases where the same C2 is used for different components (for example, corolain[.]ru).

Example malware samples and associated infrastructure

QuietSieve

Indicator
Jolotras[.]ru
Moolin[.]ru
0afce2247ffb53783259b7dc5a0afe04d918767c991db2da906277898fd80be5
e4d309735f5326a193844772fc65b186fd673436efab7c6fed9eb7e3d01b6f19

f211e0eb49990edbb5de2bcf2f573ea6a0b6f3549e772fd16bf7cc214d924824
6d4b97e74abf499fa983b73a1e6957eadb2ec6a83e206fff1ab863448e4262c6
eb1724d14397de8f9dca4720dada0195ebb99d72427703cabcb47b174a3bfea2
e4d309735f5326a193844772fc65b186fd673436efab7c6fed9eb7e3d01b6f19
b92dcbacbaaf0a05c805d31762cd4e45c912ba940c57b982939d79731cf97217
b3d68268bd4bb14b6d412cef2b12ae4f2a385c36600676c1a9988cf1e9256877
a6867e9086a8f713a962238204a3266185de2cc3c662fba8d79f0e9b22ce8dd6
a01e12988448a5b26d1d1adecc2dda539b5842f6a7044f8803a52c8bb714cdb0
8a8c1a292eeb404407a9fe90430663a6d17767e49d52107b60bc229c090a0ae9
15099fc6aea1961164954033b397d773ebf4b3ef7a5567feb064329be6236a01
137bfe2977b719d92b87699d93c0f140d659e990b482bbc5301085003c2bd58c

0e5b4e578788760701630a810d1920d510015367bf90c1eab4373d0c48a921d9	S 2
0afce2247ffb53783259b7dc5a0afe04d918767c991db2da906277898fd80be5	S 2

Pterodo

Indicator	T
gorigan[.]ru	D n
teroba[.]ru	D n
krashand[.]ru	D n
51b9e03db53b2d583f66e47af56bb0146630f8a175d4a439369045038d6d2a45	S 2
2042a2feb4d9f54d65d7579a0afba9ee1c6d22e29127991fbf34ea3da1659904	S 2
425ee82f20eb87e07a0d4f77adb72bf3377051365be203ee6ded37b399094f20	S 2
fe068e324cd4175f857dfee4c23512ed01f3abbf8b6138b715caa1ba5e9486c0	S 2
798cd714cf9e352c1e9de3d48971a366b09eeffb3513950fd64737d882c25a38	S 2
ef9b39705decbb85269518705053e7f4087758eea6bab4ba9135bf1ae922b2ea	S 2

a87e9d5e03db793a0c7b8e8e197d14745265422f05e6e50867cdfbd150d0c016	S 2
2042a2feb4d9f54d65d7579a0afba9ee1c6d22e29127991fbf34ea3da1659904	S 2
c68eb2fa929373cac727764d2cc5ca94f19a0ec7fd8c0876b98f946e72d9fa03	S 2
3b6445cf6f8e9e70cb0fff35d723fec8203375d67cbd67c9a672cddc02a7ff99	S 2
bae9895ad4e392990a09b1b8a01e424a7ad3769e538ac693919d1b99989f0cb3	S 2
c6e092316f61d2fc9c84299dd224a6e419e74c98c51a44023f8f72530ac28fdc	S 2
cb0d151d930b17f6376c18aa15fd976eac53d6f07d065fc27c40b466e3bc49aa	S 2
8ed03b1d544444b42385e79cd17c796fefae71d140b146d0757a3960d8ba3cba	S 2

Various stagers and downloaders

(DinoTrain, DilongTrash, Obfuberry, PowerPunch, DessertDown, and Obfumerry)

Indicator	Ty
%windir%\System32\schtasks.exe" /CREATE /sc minute /mo 12 /tn "deepness" /tr "wscript.exe "%PUBLIC%\Pictures\deepness.fly" //e:VBScript //b" /F	Co lir
wscript.exe C:\Users\[username]\continue.wav //e:VBScript //b	Co lir
alacritas[.]ru	Do na

libellus[.]ru	Do na
brontaga[.]ru	Do na
gortomalo[.]ru	Do na
corolain[.]ru	Do na
goloser[.]ru	Do na
delicacy[.]delicate[.]maizuko[.]ru	Do na
0f9d723c3023a6af3e5522f63f649c7d6a8cb2727ec092e0b38ee76cd1bbf1c4	SH
bf90d5db47e6ba3a1840976b6bb88a8d0dfe97dfe02c9ca31b7be4018816d232	SH
b9b41fbbd646f11d148cface520a5d4e0ec502ba85c67b00668e239082a302e3	SH
c05f4c5a6bb940e94782e07cf276fc103a6acca365ba28e7b4db09b5bbc01e58	SH
3cbe7d544ef4c8ff8e5c1e101dbdf5316d0cfbe32658d8b9209f922309162bcf	SH
3bab73a7ba6b84d9c070bb7f71daab5b40fcb6ee0387b67be51e978a47c25439	SH

ACTINIUM-owned infrastructure

Domains

The following list represents the most recent domains used by ACTINIUM as of this writing. Many of ACTINIUM's capabilities communicate with generated subdomains following the patterns discussed earlier. A list of commonly observed words in these generated names is available in the next section, although it should be noted that this list is not exhaustive.

acetica[.]online	lenatara[.]ru	oyoida[.]ru	riontos[.]ru	nerabis[.]ru
adeltorr[.]ru	ouichi[.]ru	dushnilo[.]ru	hostarama[.]ru	jokolor[.]ru
arianat[.]ru	cryptonas[.]ru	akowaika[.]ru	artisola[.]ru	nokratis[.]ru
bartion[.]ru	konoatari[.]ru	torogat[.]ru	boltorg[.]ru	machiwo[.]ru
bibliota[.]ru	moonilar[.]ru	inosokof[.]ru	draagotan[.]ru	kolotran[.]ru
bilorotka[.]ru	reapart[.]ru	holotran[.]ru	golofir[.]ru	volotras[.]ru
dokkade[.]ru	nomukou[.]ru	huskari[.]ru	goloser[.]ru	milopoda[.]ru
goshita[.]ru	mirotas[.]ru	utemomac[.]ru	gortomalo[.]ru	zerotask[.]ru
hajimari[.]ru	ismetroh[.]ru	hortoban[.]ru	gloritapa[.]ru	vasitron[.]ru
libellus[.]ru	vositra[.]ru	hopfar[.]ru	bobotal[.]ru	nopaster[.]ru
meshatr[.]ru	fartopart[.]ru	koprotas[.]ru	historap[.]ru	dangeti[.]ru

nakushita[.]ru	atasareru[.]ru	golorta[.]ru	jabilen[.]ru	haguret[.]ru
naletovo[.]ru	uzumoreru[.]ru	screato[.]ru	herumot[.]ru	klotrast[.]ru
nattanda[.]ru	sumikko[.]ru	bellinor[.]ru	saturapa[.]ru	sundabokun[.]r
nokitrav[.]ru	vivaldar[.]ru	nokata[.]ru	fortfar[.]ru	rawaumi[.]ru
nonima[.]ru	ikaraur[.]ru	nemoiti[.]ru	dudocilo[.]ru	wokoras[.]ru
onihik[.]ru	ruhodo[.]ru	mudarist[.]ru	gongorat[.]ru	yazibo[.]ru
pertolka[.]ru	asdorta[.]ru	holorta[.]ru	gortisir[.]ru	jupirest[.]ru
ruchkalo[.]ru	kolorato[.]ru	kucart[.]ru	filorta[.]ru	vostilo[.]ru
shitemo[.]ru	warau[.]ru	koltorist[.]ru	gortova[.]ru	lotorgas[.]ru
sorawo[.]ru	kimiga[.]ru	hokoldar[.]ru	amaniwa[.]ru	masshir[.]ru
telefar[.]ru	kippuno[.]ru	midiatr[.]ru	nastorlam[.]ru	martusi[.]ru
urovista[.]ru	kroviti[.]ru	bibikaro[.]ru	hilotrapa[.]ru	kovalsko[.]ru
vadilops[.]ru	hibigaru[.]ru	gribata[.]ru	alebont[.]ru	nukegaran[.]ru
zvustro[.]ru	lotorda[.]ru	vnestri[.]ru	dortisto[.]ru	

Wordlist of observed terms

ACTINIUM likely generates strings for use in various components from a wordlist. A sample of terms observed in use by ACTINIUM can be found below. ACTINIUM has been observed to use these terms for:

- Subdomains for their C2 infrastructure
- Scheduled task names
- Folder names
- Malware file names

ACTINIUM also likely generates strings for other uses where they attempt to disguise their activities.

abrupt	allegiance	allen	alley	allied	allo
allow	allowance	allowing	allows	alloy	allu
ally	almond	almost	alongside	alphabet	alre
alter	alteration	although	always	am	ama
amber	ambitious	amends	amid	among	beve
beware	beyond	bicycle	big	bigger	bike
bikes	bill	billion	claimed	clank	clap
clash	clasped	classes	classroom	cough	coul
councilman	countenance	counteract	countries	country	cour
courageous	cronos	debts	deceive	deceived	dece
deception	decide	decided	decidedly	decision	deci
deck	declaration	declare	declared	decline	decl
decoy	decrease	decree	decrepit	dedicate	dedu
deed	deep	deeper	deep-going	deep-green	deep

deep-grounded	deep-grown	deephaven	deepish	deep-kiss	deep
deep-laid	deeplier	deep-lunged	deeply	deep-lying	deep
deep-musing	deep-naked	deepnesses	deep-persuading	deep-piled	deep
deep-pondering	deep-premeditated	deep-read	deep-revolving	deep-rooted	deep
deep-sea	deep-searching	deep-seated	deep-seatedness	deep-set	deep
deep-sighted	deep-sinking	deep-skirted	deepsome	deep-sore	deep
deep-sunken	deep-sweet	deep-tangled	deep-throated	deep-toned	deep tran
deep-troubled	deep-vaulted	deep-versed	deep-voiced	deep-water	deep
deepwatermen	deep-worn	deep-wounded	deer	deerberry	deer
deerdog	deerdre	deere	deerflies	deerflys	deer
deerhorn	deering	deerlet	deer-mouse	deers	deer
deery	deeryards	default	defeated	defect	defe
defence	defend	defense	defensive	defiance	defia
deficiency	defined	definite	definitely	defy	degr
degree	deity	dejected	delay	delayed	dele
deliberate	deliberately	delicious	delight	delighted	delig
delirium	deliverance	delivered	delivery	deluge	delv
demand	demanded	demolition	demonstrate	demonstration	den
dene	denial	denied	denote	dense	dent
deny	depart	departed	department	departments	depa
depended	dependent	deplore	deploy	deployment	depr
depth	depths	deputy	derisive	derived	des
descendant	descended	descent	describe	description	dese
deserter	deserts	deserve	deserves	design	desi
designer	designs	desire	desolate	despair	desp
desperately	despise	despite	dessert	destitute	dest
destroyer	detach	detached	detail	endanger	endi
endless	endlessly	endure	enemies	energy	enfo
faithless	fake	falcon	fame	familiar	fami
famous	fan	fancied	gleaming	glide	glim
gloom	gloomy	glory	glossy	gloves	glow

glue	gnaw	goat	goes	integer	integ
intelligence	intelligent	intend	descendant	descended	desc
describe	description	desert	interested	interesting	inter
island	isolation	issue	issued	its	itsel
jack	jackal	jacket	jackson	jake	jam
james	jan	january	jar	jaw	jaws
jazz	jealous	jealousy	jean	jeanne	jean
jeer	jeff	jelly	jerk	jersey	jeru
jessamy	jessie	jest	jet	jew	jewe
jeweller	jewellery	jewels	jill	joan	job
jobs	joe	join	joining	joint	joke
joking	jolly	jonas	joseph	josephine	josie
joy	joyful	joyfully	judge	judgment	jug
juice	juicy	july	jumble	jumped	jum
june	jungle	junior	junk	just	justl
juvenile	lover	low	lower	loyalty	luck
lucy	luggage	luke	lumber	lump	lunc
luncheon	lustre	luxurious	luxury	mankind	man
mansion	margaret	margarita	margin	marriage	mar
masquerade	naturally	nature	naughty	navigation	navy
nay	near	neat	necessarily	necklace	ned
needle	needlework	neglect	parlor	parlour	parr
parsley	participate	parties	parting	penknife	per
perceive	percent	percy	perfect	perform	perf
perfume	pleasantly	pressure	presume	pretence	pret
pretty	prevail	prevailed	prevhost	prey	price
priest	primary	prince	princess	printing	pum
punctual	punish	punishment	pupil	purchase	purc
pure	purge	purpose	purse	pursuing	refe
reflected	regions	registered	registration	registry	regr
regular	regularly	regulate	reject	relations	relat
relax	release	reliable	salary	sale	salm
salt	salts	salvation	same	sand	scar
scarcely	scared	scarf	scarlet	scattered	scen
scenery	scenes	scent	scheme	scholars	scho
science	scold	scope	scorn	scornful	scou

scout	scowled	shoe	shone	shooting	sorti
sought	sound	sounding	soup	sour	sour
stool	stoop	stooped	stop	stopped	stop
storm	stout	strawberries	stream	strengthen	stret
strict	striking	string	strings	striped	strip
stroke	stroll				

NOTE: These indicators should not be considered exhaustive for this observed activity.

Detections

Microsoft 365 Defender

Microsoft Defender Antivirus

- Trojan:MSIL/QuietSieve.Gen!dha
- TrojanDownloader:VBS/ObfuMerry.A!dha
- TrojanDownloader:VBS/ObfuBerry.A!dha
- TrojanDropper:Win32/PowerPunch.A!dha
- TrojanDropper:Win32/DinoTrain.gen!dha
- TrojanDownloader:VBS/DessertDown.A!dha
- TrojanDownloader:VBS/DessertDown.B!dha
- TrojanDownloader:Win32/DilongTrash!dha
- TrojanDownloader:Win32/PterodoGen.A!dha
- TrojanDownloader:Win32/PterodoGen.B!dha
- TrojanDownloader:Win32/PterodoGen.C!dha

Microsoft Defender for Endpoint

Alerts with the following titles in the security center can indicate threat activity on your network:

- ACTINIUM activity group

The following alerts might also indicate threat activity associated with this threat. These alerts, however, may be triggered by unrelated threat activity. We're listing them here because we recommend that these alerts be investigated and remediated immediately given the severity of the attacks.

- Suspicious obfuscation or deobfuscation activity
- Suspicious script execution
- A script with suspicious content was observed
- PowerShell dropped a suspicious file on the machine
- Anomalous process executing encoded command
- Suspicious dynamic link library loaded
- An anomalous scheduled task was created
- An uncommon file was created and added to a Run Key
- Suspicious screen capture activity
- Staging of sensitive data
- Suspicious process transferring data to external network

Microsoft Defender for Office 365

Microsoft Defender for Office 365 customers can use the email entity page to search for and visualize the potential impact of these attacks to your organization.

The following email security alerts may indicate threat activity associated with this threat. These alerts, however, may be triggered by unrelated threat activity. We're listing them here because we recommend that these alerts be investigated and remediated immediately given the severity of the attacks.

- Email messages containing malicious file removed after delivery
- Email messages containing malware removed after delivery
- Email messages removed after delivery
- Email reported by user as malware or phish
- Malware campaign detected after delivery
- Malware campaign detected and blocked
- Malware not zapped because ZAP is disabled

Advanced hunting queries

Microsoft Sentinel

To locate possible ACTINIUM activity mentioned in this blog post, Microsoft Sentinel customers can use the queries detailed below:

Identify ACTINIUM IOCs

This query identifies a match across various data feeds for IOCs related to ACTINIUM:

https://github.com/Azure/Azure-Sentinel/blob/master/Detections/MultipleDataSources/ActiniumFeb2022.yaml

Identify antivirus detection of ACTINIUM activity

This query identifies a match in the Security Alert table for Microsoft Defender Antivirus detections related to the ACTINIUM actor:

https://github.com/Azure/Azure-Sentinel/blob/master/Detections/SecurityAlert/ActiniumAVHits.yaml

Microsoft 365 Defender

To locate related activity, Microsoft 365 Defender customers can run the following advanced hunting queries:

Find ACTINIUM-related emails

Use this query to look for look for emails that may have been received in your environment related to ACTINIUM.

```
EmailEvents
| where SenderMailFromDomain =~ 'who-int.info'
    or SenderFromDomain =~ 'who-int.info'
```

Surface ACTINIUM-related alerts

Use this query to look for alerts related to ACTINIUM alerts.

```
AlertInfo
| where Title in~('ACTINIUM activity group')
```

Surface devices with ACTINIUM related alerts and gather additional device alert information

Use this query to look for threat activity associated with ACTINIUM alerts.

```
// Get any devices with ACTINIUM related Alert Activity
let DevicesACTINIUMAlerts = AlertInfo
| where Title in~('ACTINIUM activity group')
// Join in evidence information
| join AlertEvidence on AlertId
| where DeviceId != ""
| summarize by DeviceId, Title;
// Get additional alert activity for each device
AlertEvidence
| where DeviceId in(DevicesACTINIUMAlerts)
// Add additional info
| join kind=leftouter AlertInfo on AlertId
| summarize DeviceAlerts = make_set(Title), AlertIDs =
make_set(AlertId) by DeviceId, bin(Timestamp, 1d)
```

Surface suspicious MSHTA process execution

Use this query to look for MSHTA launching with command lines referencing DLLs in the AppData\Roaming path.

```
DeviceProcessEvents
| where FileName =~ "mshta.exe"
| where ProcessCommandLine has_all (".dll", "Roaming")
| where ProcessCommandLine contains @"Roaming\j"
| extend DLLName = extract(@"[jJ][a-z]{1,12}\.dll", 0,
ProcessCommandLine)
```

Surface suspicious Scheduled Task activity

Use this query to look for Scheduled Tasks that may relate to ACTINIUM activity.

```
DeviceProcessEvents
| where ProcessCommandLine has_all ("schtasks.exe", "create",
"wscript", "e:vbscript", ".wav")
```

Related Posts

Research Threat intelligence Microsoft Defender Threat actors ·

Research Threat intelligence Microsoft Copilot for Security

Apr 22 · 10 min read

Analyzing Forest Blizzard’s custom post-compromise tool for exploiting CVE-2022-38028 to obtain credentials

Since 2019, Forest Blizzard has used a custom post-compromise tool to exploit a vulnerability in the Windows Print Spooler service that allows elevated permissions. Microsoft has issued a security update addressing this vulnerability as CVE-2022-38028.

Threat actors

Feb 14 · 13 min read

Staying ahead of threat actors in the age of AI

Microsoft, in collaboration with OpenAI, is publishing research on emerging threats in the age of AI, focusing on identified activity associated with known threat actors Forest Blizzard, Emerald Sleet, Crimson Sandstorm, and others. The observed activity includes prompt-injections, attempted misuse of large language models (LLM), and fraud.

Research Threat intelligence Microsoft Defender Threat actors ·

Dec 7, 2023 · 28 min read

Star Blizzard increases sophistication and evasion in ongoing attacks

Microsoft Threat Intelligence continues to track and disrupt malicious activity attributed to a Russian state-sponsored actor we track as Star Blizzard, who has continuously improved their detection evasion capabilities while remaining focused on email credential theft against targets.

Research Threat intelligence Threat actors ·

Nov 9, 2023 · 6 min read

Microsoft shares threat intelligence at CYBERWARCON 2023

At the CYBERWARCON 2023 conference, Microsoft and LinkedIn analysts are presenting several sessions detailing analysis across multiple sets of threat actors and related activity, demonstrating Microsoft Threat Intelligence’s ongoing efforts to track threat actors, protect customers, and share information with the wider security community.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Connect with us on social

What's new Microsoft Store Education

Surface Pro

Surface Laptop

Surface Laptop Studio 2

Surface Laptop Go 3

Microsoft Copilot

AI in Windows

Explore Microsoft products

Windows 11 apps

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Microsoft 365 Copilot

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy

Sitemap Contact Microsoft Privacy Manage cookies Terms of use Trademarks Safety & eco Recycling About our ads