Threat Analysis Group

Exposing initial access broker with ties to Conti

Mar 17, 2022

6 min read

Share Twitter Facebook Linkedin Mail Copy link V Vlad Stolyarov Threat Analysis Group B Benoit Sevens Threat Analysis Group Share Twitter Facebook Linkedin Mail Copy link

In early September 2021, Threat Analysis Group (TAG) observed a financially motivated threat actor we refer to as EXOTIC LILY, exploiting a 0day in Microsoft MSHTML (CVE-2021-40444). Investigating this group's activity, we determined they are an Initial Access Broker (IAB) who appear to be working with the Russian cyber crime gang known as FIN12 (Mandiant, FireEye) / WIZARD SPIDER (CrowdStrike).

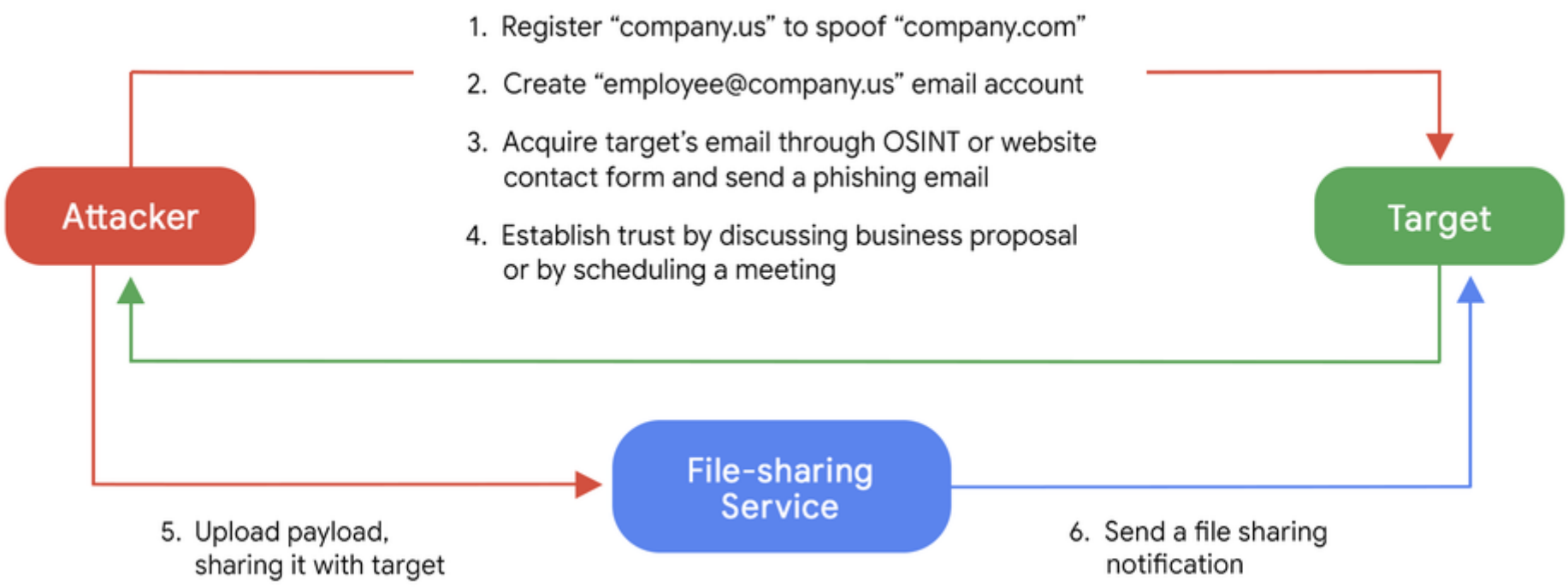
Initial access brokers are the opportunistic locksmiths of the security world, and it's a full-time job. These groups specialize in breaching a target in order to open the doors——or the Windows——to the malicious actor with the highest bid.

EXOTIC LILY is a resourceful, financially motivated group whose activities appear to be closely linked with data exfiltration and deployment of human-operated ransomware such as Conti and Diavol. At the peak of EXOTIC LILY's activity, we estimate they were sending more than 5,000 emails a day, to as many as 650 targeted organizations globally. Up until November 2021, the group seemed to be targeting specific industries such as IT, cybersecurity and healthcare, but as of late we have seen them attacking a wide variety of organizations and industries, with less specific focus.

We have observed this threat actor deploying tactics, techniques and procedures (TTPs) that are traditionally associated with more targeted attacks, like spoofing companies and employees as a means of gaining trust of a targeted organization through email campaigns that are believed to be sent by real human operators using little-to-no automation. Additionally and rather uniquely, they leverage legitimate file-sharing services like WeTransfer, TransferNow and OneDrive to deliver the payload, further evading detection mechanisms. This level of human-interaction is rather unusual for cyber crime groups focused on mass scale operations.

Spoofing Organizations and Identities

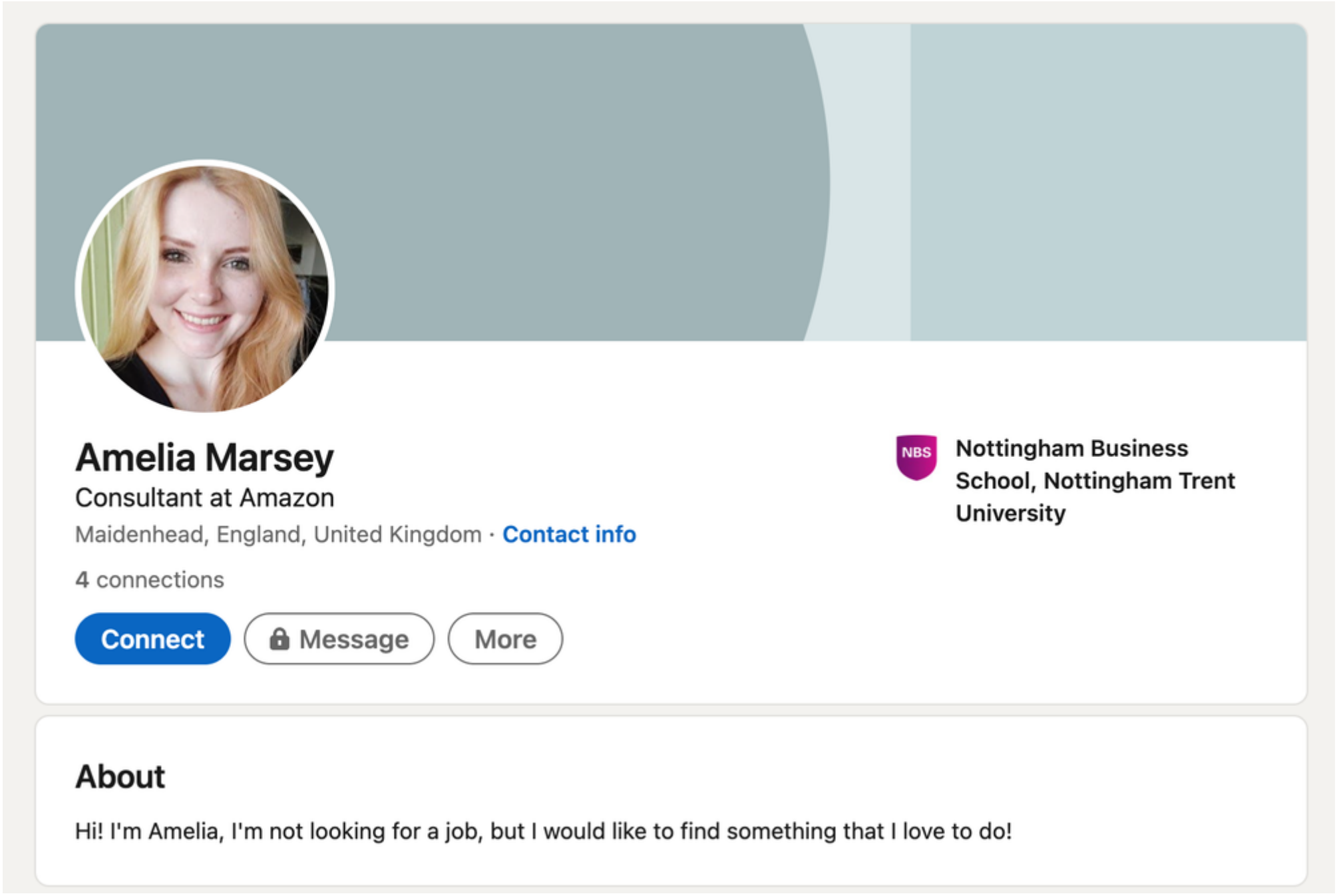
EXOTIC LILY's attack chain has remained relatively consistent throughout the time we've been tracking the group:



One notable technique is the use of domain and identity spoofing as a way of gaining additional credibility with a targeted organization. In the majority of cases, a spoofed domain name was identical to a real domain name of an existing organization, with the only difference being a change of TLD to ".us", ".co" or ".biz".

Initially, the group would create entirely fake personas posing as employees of a real company. That would sometimes consist of creating social media profiles, personal websites and generating a fake profile picture using a public service to create an AI-generated human face. In November 2021, the

group began to impersonate real company employees by copying their personal data from social media and business databases such as RocketReach and CrunchBase.



One of the fake social media profiles created by EXOTIC LILY

Using spoofed email accounts, attackers would then send spear phishing emails under the pretext of a business proposal, such as seeking to outsource a software development project or an information security service.

Hi!

Our company is currently interested in your services and products for our upcoming project. We are one of the leading highway and bridge construction contractors. We provide best-in-class engineering and construction services with the upmost quality. We're looking forward to starting our new project with your assistance. Could we discuss whether you can provide us with a suitable quote?

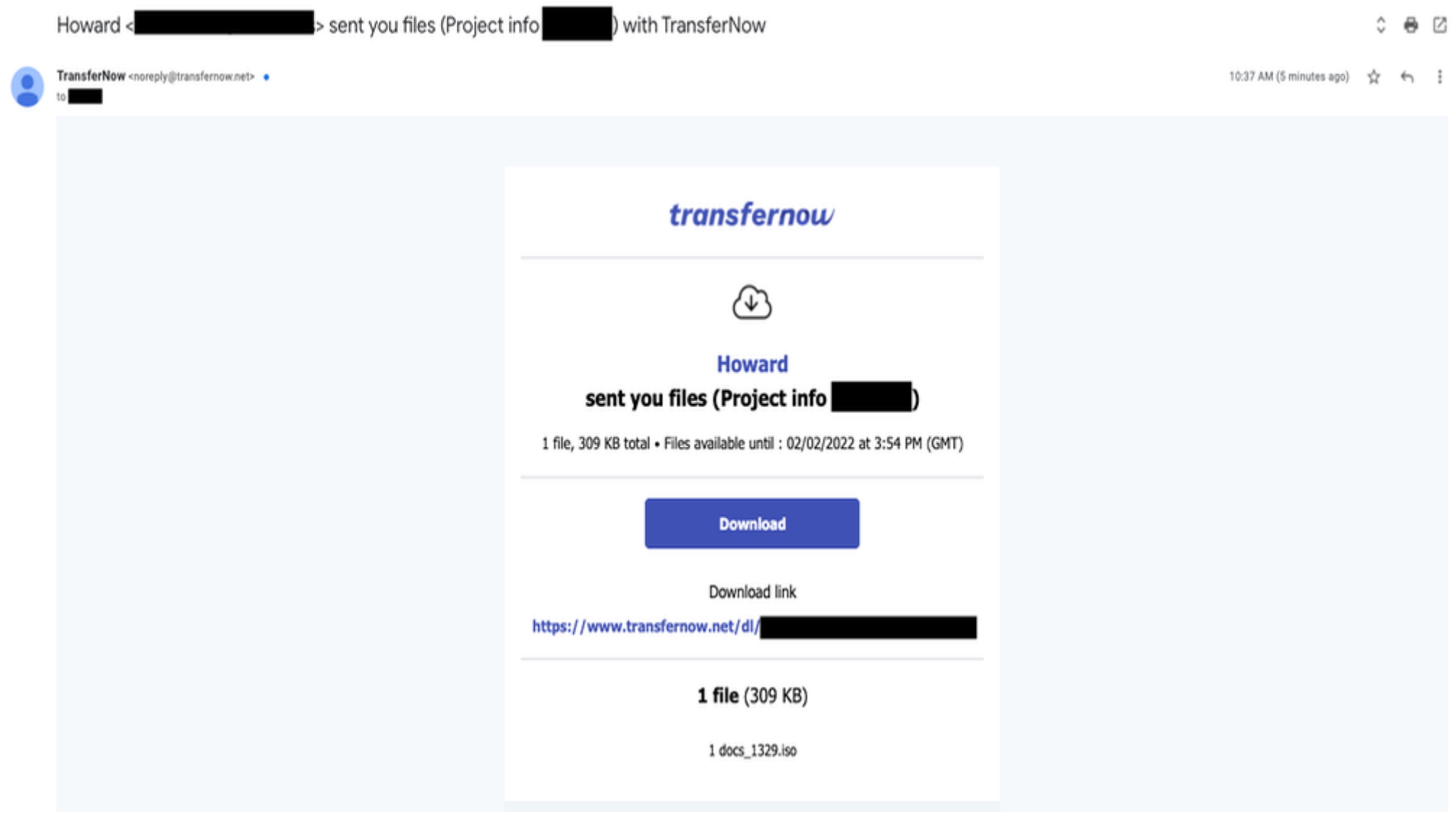
Regards,

Erik [redacted]
Project Manager
Mobile: +1-[redacted]51
Email: erik[redacted]@halmarinternational.com

Example of an EXOTIC LILY phishing email impersonating as an employee of a legitimate company

Attackers would sometimes engage in further communication with the target by attempting to schedule a meeting to discuss the project's design or requirements.

At the final stage, the attacker would upload the payload to a public file-sharing service (TransferNow, TransferXL, WeTransfer or OneDrive) and then use a built-in email notification feature to share the file with the target, allowing the final email to originate from the email address of a legitimate file-sharing service and not the attacker’s email, which presents additional detection challenges.



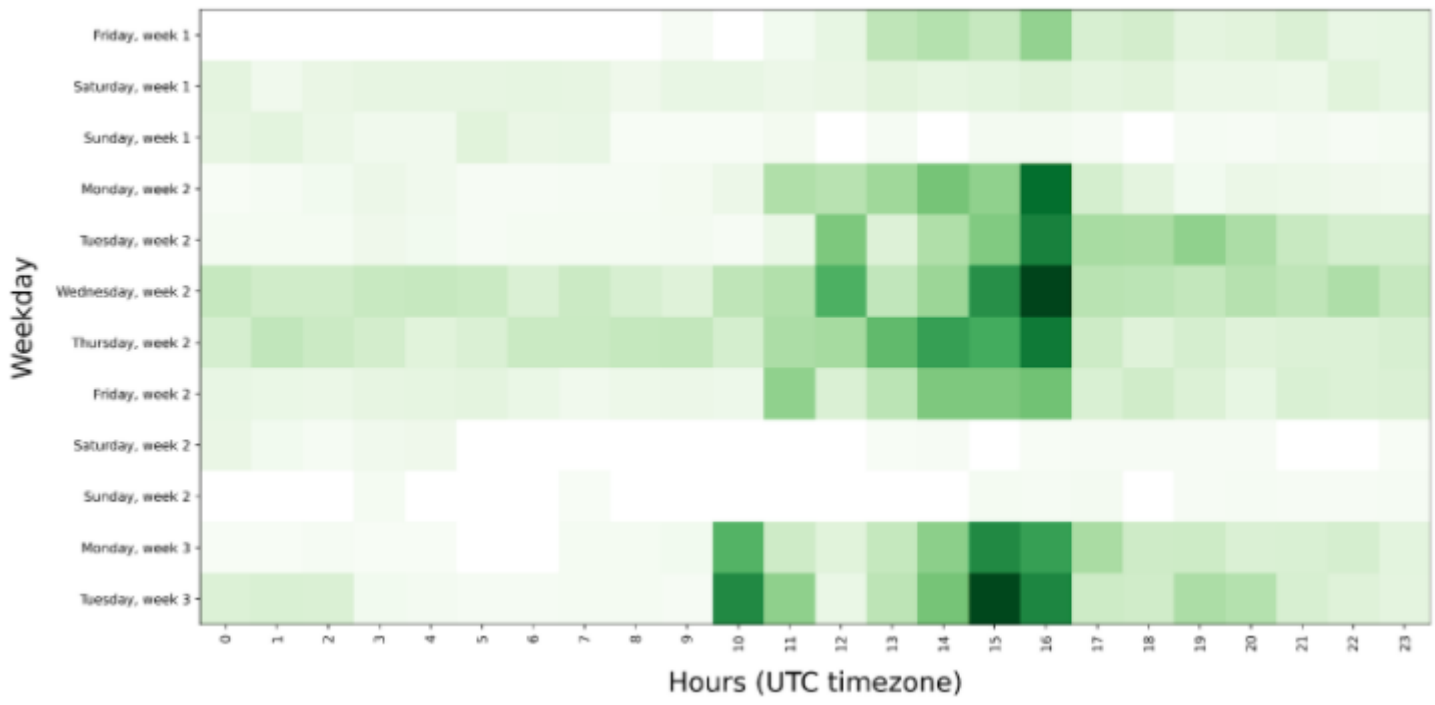
Attacker uses a file-sharing service email notification feature to send BazarLoader ISO payload

Human-Operated Phishing at Scale

Further evidence suggests an operator's responsibilities might include:

- customizing the initial "business proposal" templates when first reaching out to a targeted organization;
- handling further communications in order to gain affinity and trust;
- uploading malware (acquired from another group) to a file-sharing service prior to sharing it with the target.

A breakdown of the actor's communication activity shows the operators are working a fairly typical 9-to-5 job, with very little activity during the weekends. Distribution of the actor's working hours suggest they might be working from a Central or an Eastern Europe timezone.



Breakdown of actor's communication activity. Deeper color indicates more activity.

Malware and Attribution

Although the group came to our attention initially due to its use of documents containing an exploit for CVE-2021-40444, they later switched to the delivery of ISO files with hidden BazarLoader DLLs and LNK shortcuts. These samples have some indicators that suggest they were custom-built to be used by the group. For example, metadata embedded in the LNK shortcuts shows that a number of fields, such as the "Machine Identifier" and "Drive

Serial Number" were shared with BazarLoader ISOs distributed via other means, however other fields such as the command line arguments were unique for samples distributed by EXOTIC LILY.

```
Local path: C:\Windows\System32\cmd.exe
Command line arguments: /c xcopy /y DumpStack.log c:\programdata\ &&
C:\Windows\System32\rundll32.exe C:\programdata\DumpStack.log,sploaд && exit
Icon location: %systemroot%\system32\imageres.dll

Drive serial number: 0xa6405015
Machine identifier: windev2106eval
```

In March, the group continued delivering ISO files, but with a DLL containing a custom loader which is a more advanced variant of a first-stage payload previously seen during CVE-2021-40444 exploitation. The loader can be recognized by its use of a unique user-agent "bumblebee" which both variants share. The malware, hence dubbed BUMBLEBEE, uses WMI to collect various system details such as OS version, user name and domain name, which are then exfiltrated in JSON format to a C2. In response, it expects to receive one of the several supported "tasks", which include execution of shellcode, dropping and running executable files. At the time of the analysis, BUMBLEBEE was observed to fetch Cobalt Strike payloads.

EXOTIC LILY activities overlap with a group tracked as DEV-0413 (Microsoft) and were also described by Abnormal in their recent post. Earlier reports of attacks exploiting CVE-2021-40444 (by Microsoft and other members of the security community) have also indicated overlaps between domains involved in the delivery chain of an exploit and infrastructure used for BazarLoader and Trickbot distribution.

We believe the shift to deliver BazarLoader, along with some other indicators such as a unique Cobalt Strike profile (described by RiskIQ) further confirms the existence of a relationship between EXOTIC LILY and actions of a Russian cyber crime group tracked as WIZARD SPIDER (CrowdStrike), FIN12 (Mandiant, FireEye) and DEV-0193 (Microsoft). While the nature of those relationships remains unclear, EXOTIC LILY seems to operate as a separate entity, focusing on acquiring initial access through email campaigns, with follow-up activities that include deployment of Conti and Diavol ransomware, which are performed by a different set of actors.

Improving User Protection

As part of our efforts to combat serious threat actors, we use results of our research to improve the safety and security of our products. In collaboration with Gmail and Safe Browsing, we are improving protections by adding additional warnings for emails originating from website contact forms, better identification of spoofing, and adjusting the reputation of email file sharing notifications. Additionally, we're working with Google's CyberCrime Investigation Group to share relevant details and indicators with law enforcement.

TAG is committed to sharing our findings as a way of raising awareness with the security community, and with companies and individuals that might have been targeted or suffered from this threat actor's activities. We hope that improved understanding of the group's tactics and techniques will enhance threat hunting capability and lead to stronger user protections across industry.

Indicators of Compromise (IOCs)

Recent domains used in email campaigns:

- conlfex[.]com
- avrobio[.]co
- elemblo[.]com
- phxmfg[.]co
- modernmeadow[.]co
- lsoplexis[.]com
- craneveyor[.]us
- faustel[.]us
- lagauge[.]us
- missionbio[.]us
- richllndmetals[.]com
- kvnational[.]us
- prmflltration[.]com
- brightlnsight[.]co
- belcolnd[.]com

- awsblopharma[.]com
- amevida[.]us
- revergy[.]us
- al-ghurair[.]us
- opontia[.]us

BazarLoader ISO samples:

- 5ceb28316f29c3912332065eeaaebf59f10d79cd9388ef2a7802b9bb80d797be
- 9fdec91231fe3a709c8d4ec39e25ce8c55282167c561b14917b52701494ac269
- c896ee848586dd0c61c2a821a03192a5efef1b4b4e03b48aba18eedab1b864f7

Recent BUMBLEBEE ISO samples:

- 9eacade8174f008c48ea57d43068dbce3d91093603db0511467c18252f60de32
- 6214e19836c0c3c4bc94e23d6391c45ad87fdd890f6cbd3ab078650455c31dc8
- 201c4d0070552d9dc06b76ee55479fc0a9dfacb6dbec6bbec5265e04644eebc9
- 1fd5326034792c0f0fb00be77629a10ac9162b2f473f96072397a5d639da45dd
- 01cc151149b5bf974449b00de08ce7dbf5eca77f55edd00982a959e48d017225

Recent BUMBLEBEE C2:

- 23.81.246[.]187:443

POSTED IN: