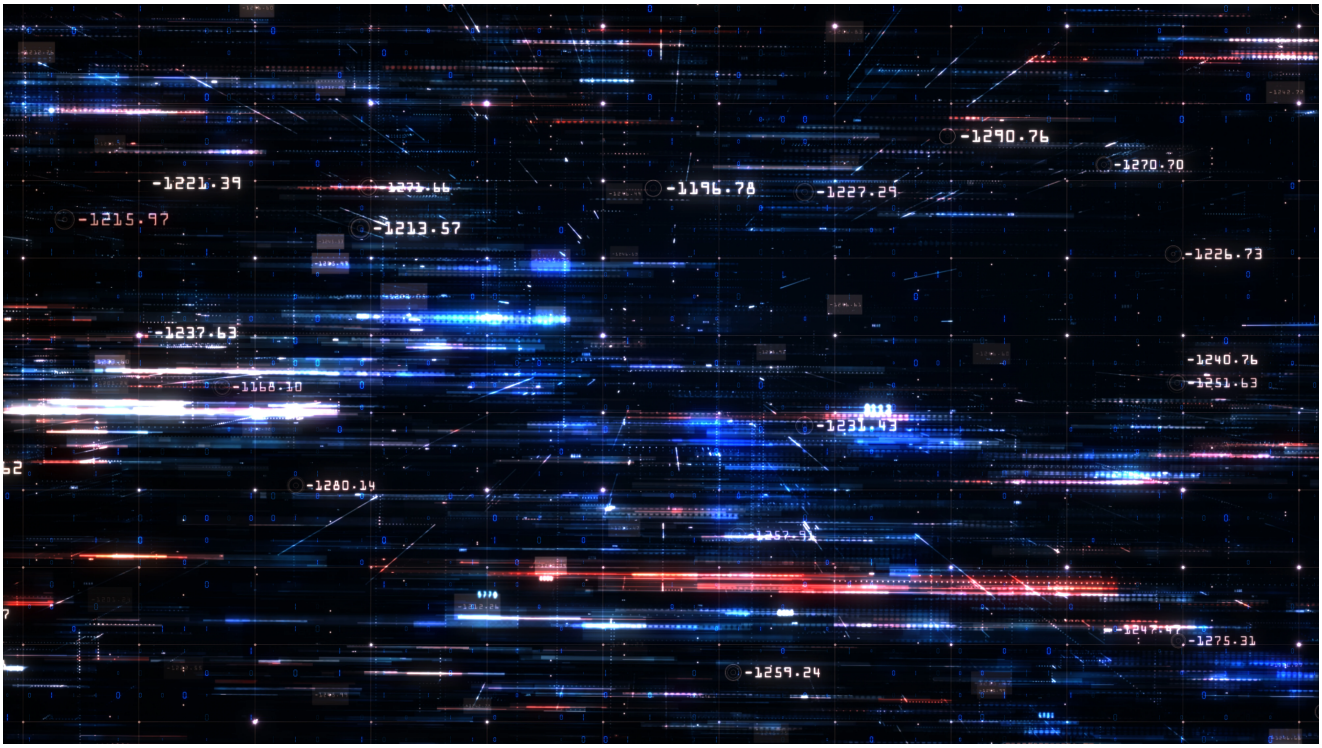
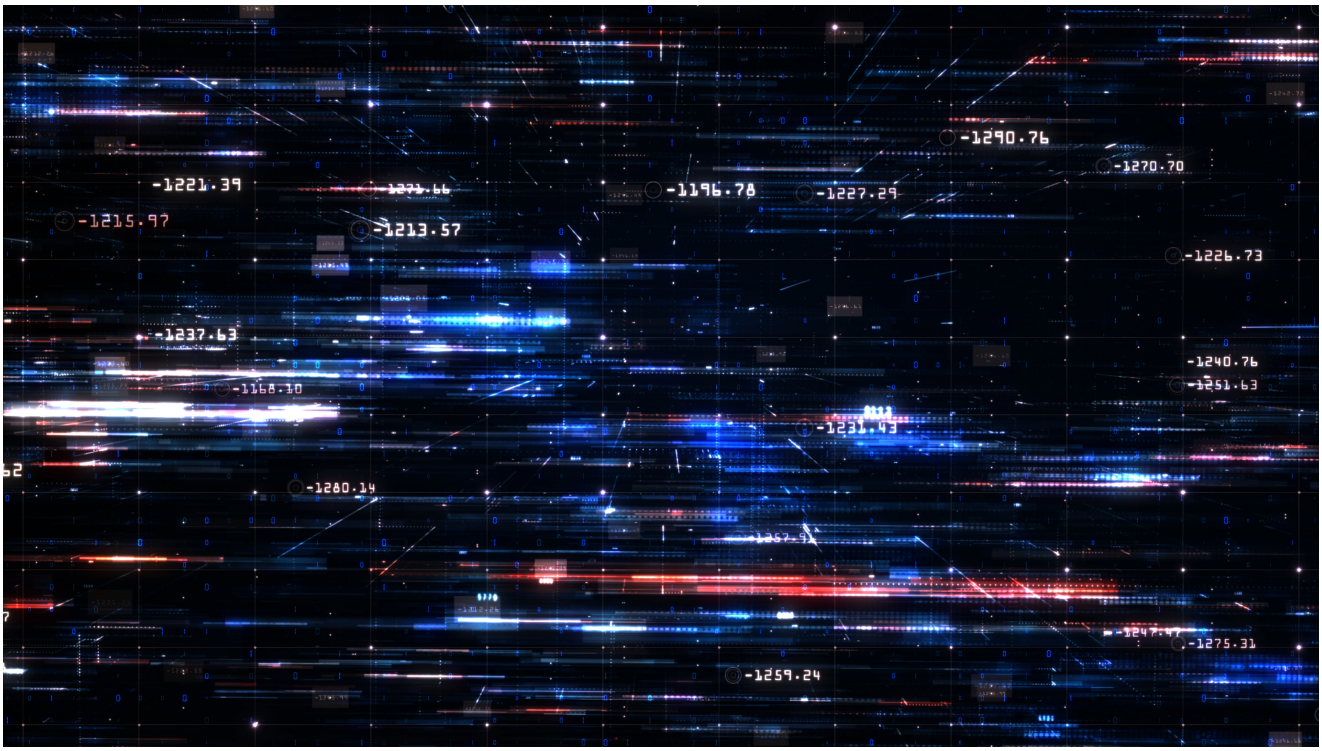
Detecting a MUMMY SPIDER campaign and Emotet infection

ironnet.com/blog/detecting-a-mummyspider-campaign-and-emotet-infection

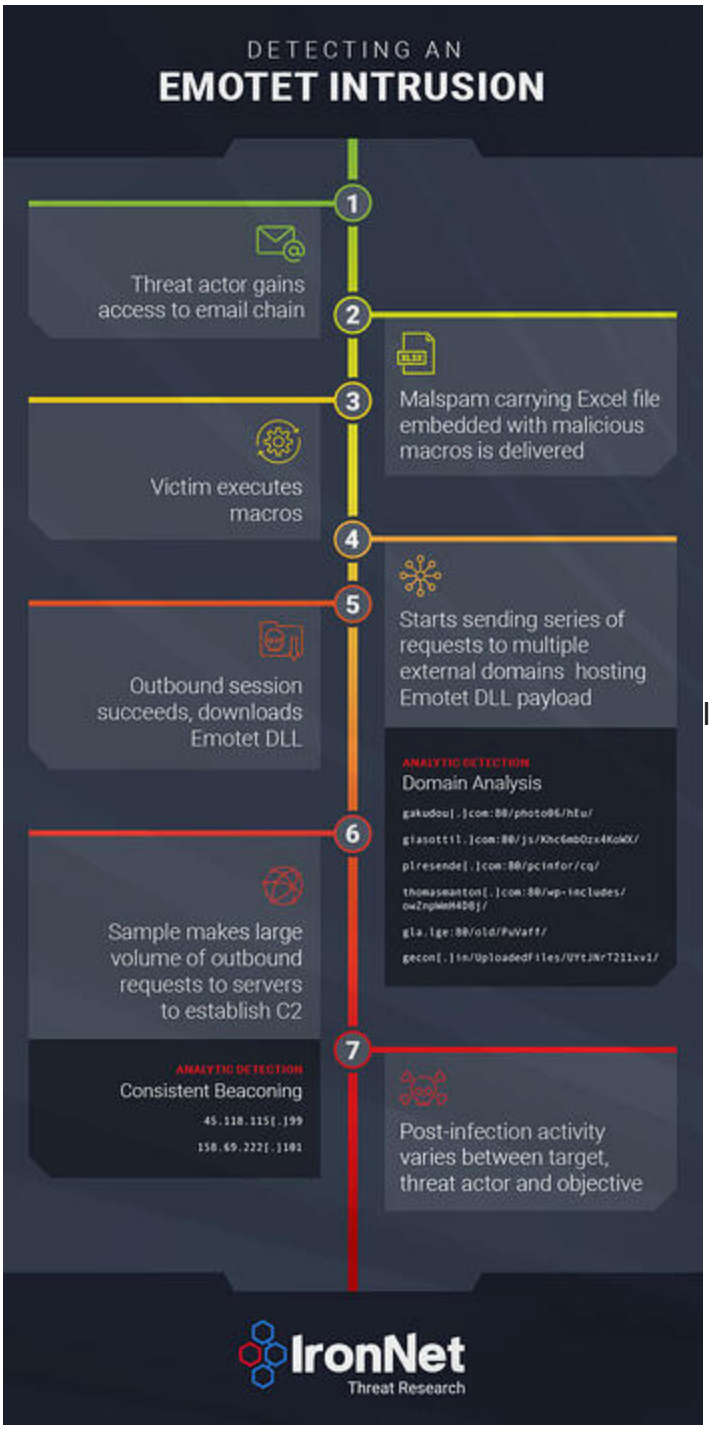




May 11, 2022

Key findings:

- At the start of the Eid Al-Fitr (Islamic holiday) weekend in early May 2022, IronNet Threat Research detected a thread hijacking attack carrying Emotet malware against an organization located in the Asia Pacific region.
- This cyber attack is likely part of a new campaign by the MUMMY SPIDER threat group, designed to test a new bypass for Microsoft disabling macros by default for use in future large-scale campaigns.
- This finding supports recent open-source reporting that MUMMY SPIDER has begun to conduct more targeted operations, and it is likely the threat actors will continue to use their access to enterprise emails to conduct further phishing attacks.



IronNet's Network Detection and Response (NDR) platform, in combination with our cybersecurity experts, detected an Emotet infection in the network of a customer located in the Asia Pacific region at the start of the Eid Al-Fitr (Islamic holiday) weekend in early May 2022. We were able to detect the aftermath of a successful phishing attack against an employee at the company, which resulted in an infection of a host in the client enterprise by Emotet malware. While we are still working with our partner to assist in triage and remediation, we wanted to share our findings to increase the communities ability to collectively defend against these types of attacks. We posit that this attack is part of a new campaign by the MUMMY SPIDER threat group, designed to test updated techniques, tactics, and procedures (TTP) for future campaigns.

This article discusses the threat group behind the attack and breaks down the post-compromise activity that occurred within the client enterprise. This attack bypassed the client enterprise's anti-virus protection and security products; however, IronNet's behavioral analytics were able to detect the post-compromise activity and quickly alert the customer to the infection.

MUMMY SPIDER returns

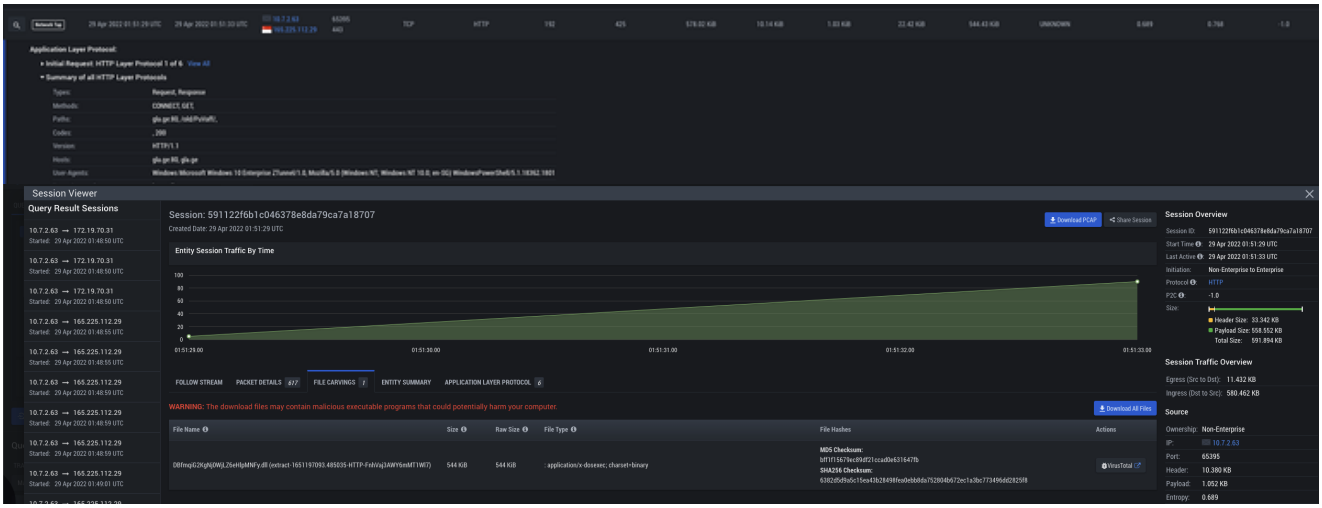
MUMMY SPIDER (also known as TA54) is a threat group that utilizes various malicious spam (malspam) email campaigns to deploy Emotet malware. First detected in 2014, Emotet is a modular, polymorphic trojan that is capable of evading signature-based detection and spreading throughout a victim network to compromise additional systems. Emotet often serves as a first–or second–stage malware that can drop and download further payloads, which could ultimately lead to data theft, remote control of systems, financial losses, and operational disruptions. An international law enforcement effort succeeded in taking down the Emotet botnet in 2021, but it has since resurfaced with a new focus on targeted attacks rather than the previous "spray and pray" tactics it was once known for. We cannot claim with absolute certainty that the group is linked to Russia; however, on April 20th 2022, a joint alert issued by cybersecurity agencies from Australia, Canada, New Zealand, the U.S., and the U.K. mentioned the MUMMY SPIDER threat group when warning organizations of the threat of Russian cyber attacks on critical infrastructure.

Unlike most threat groups, MUMMY SPIDER operates atypically; they will hibernate for months at a time and conduct operations in short bursts over a several month period. Additionally, recent reports attributed to this group have coincided with holiday seasons. Historically, when the group resumed operations, they utilized new variants of Emotet in an attempt to bypass security efforts. In the case of the compromise detailed in this article, we believe that the MUMMY SPIDER threat group may have been testing a new bypass for Microsoft disabling macros by default. This capability involves using OneDrive URLs or XLL files instead of traditional macro-enabled documents.ProofPoint believes that the reason for the lower-than-normal target volume is because MUMMY SPIDER is testing the success of this new technique before adopting it on a larger scale.

Behavioral detection and incident analysis

On April 29th, 2022, at 0100UTC, an enterprise user received a phishing email with a zip file attached. The archive contained an XLL file that the victim accidentally executed on the host computer. This triggered a series of requests to multiple external domains, which hosted the new Emotet malware. While a majority of these outbound requests were blocked by enterprise security products, an outbound session succeeded to `gla[.]ge:80/old/PuVaff/` at 0151UTC and a DLL (Emotet) was downloaded. The sample was not flagged as malicious by VirusTotal at the time of detection. IronNet observed the host making a large volume of outbound requests to various remote servers in an

attempt to establish command and control (C2) communications. Similar to the domain requests, a majority of these attempts were blocked, but a small number were successful. IronDefense was able to generate alerts based on the anomalous nature of the domains, two instances of C2 beaconing activity, and numerous threat-intelligence-based alerts.



After reporting this activity to the customer, we were informed that the attack occurred on the Friday before a major holiday weekend; this suggests a potential attack of opportunity, which corroborates with the new TTP that MUMMY SPIDER is assumed to be operating under. IronNet was able to alert the customer shortly after their workday ended Friday, enabling isolation of the infected host and mitigation during the long weekend. There is no evidence of lateral movement attempts from the infected host, supporting the assessment that this was isolated and thus part of MUMMY SPIDER's new test campaign model.

Thread Hijacking

After initial triage, IronNet's threat hunters and intel analysts requested a copy of the phishing email used and were able to categorize this as a thread hijacking attack. Thread Hijacking is a process in which a threat actor compromises and injects themselves into an email thread in an effort to increase legitimacy and trust. In this instance, the actors leveraged an email chain that involved updating a spreadsheet of delivery information, providing a legitimate use case for the phishing target to open the attached file. While the sender's address was not from a legitimate enterprise domain, the email was able to avoid suspicion from the user.

When we categorized this as a thread hijacking attack, we uncovered additional concerns that we began to investigate. Palo Alto released an article in 2020 detailing this type of attack, which indicates the post-infection goal is exfiltrating host data via C2. This discovery suggests the enterprise user was likely targeted, evidenced by the email being sent specifically to the user. We were able to use this information to inform the customer that

there were likely additional infections of one or more personnel from the original email chain, making them aware of additional thread hijacking attacks that would be likely using emails from the victim user.

IronNet conducted a review of indicators of compromise (IOC) associated with recent MUMMY SPIDER campaigns and identified external scanning attempts against several enterprise customers. While most of these appeared to be generic scanning, one instance involved a large volume of scanning against customer Simple Mail Transfer Protocol (SMTP) servers. We conclude this was likely an attempt to identify more malspam targets. IronNet has since deployed Threat Intelligence Rules (TIR) and propagated the incident alerts throughout the IronDome, enabling other IronNet customers to have increased detection capability and reduced response time through collective defense.

Conclusion

Recent reporting indicates that MUMMY SPIDER and other actors that use Emotet have begun to conduct more targeted operations, increasing the likelihood of spear-phishing against enterprise employees. While preventing all enterprise users from being the victim of a phishing attack would be ideal, it is statistically unlikely. Awareness training is recommended and effective, but having additional layers of security in the event of compromise is critical. This incident highlights the importance of behavioral detections as threat actors work to evade traditional security tools and signature-based detections. IronNet's ability to detect the behavioral aspects of this attack prevented the threat group from having extended access to the customer's enterprise over a long weekend and potentially causing further damage.

IOCs

URLs:

- `gakudou[.]com:80/photo06/hEu/`
- `giasotti[.]com:80/js/Khc6mb0zx4KoWX/`
- `plresende[.]com:80/pcinfor/cq/`
- `thomasmanton[.]com:80/wp-includes/owZnpWmH4D8j/`
- `gla[.]ge:80/old/PuVaff/`
- `gccon[.]in/UploadedFiles/UYtJNrT2llxy1/`

Extract from C2 Config via Tria.ge

- `176.31.73.90:443`
- `45.76.159.214:8080`
- `138.197.147.101:443`
- `104.168.154.79:8080`
- `149.56.131.28:8080`

- `5.9.116.246:8080`
- `77.81.247.144:8080`
- `172.104.251.154:8080`
- `50.30.40.196:8080`
- `173.212.193.249:8080`
- `51.91.76.89:8080`
- `197.242.150.244:8080`
- `103.75.201.2:443`
- `51.254.140.238:7080`
- `79.137.35.198:8080`
- `72.15.201.15:8080`
- `27.54.89.58:8080`
- `189.126.111.200:7080`
- `196.218.30.83:443`
- `82.165.152.127:8080`
- `164.68.99.3:8080`
- `183.111.227.137:8080`
- `167.172.253.162:8080`
- `153.126.146.25:7080`
- `129.232.188.93:443`
- `151.106.112.196:8080`
- `188.44.20.25:443`
- `167.99.115.35:8080`
- `134.122.66.193:8080`
- `185.4.135.165:8080`
- `212.24.98.99:8080`
- `51.91.7.5:8080`
- `146.59.226.45:443`
- `131.100.24.231:80`
- `212.237.17.99:8080`
- `201.94.166.162:443`
- `45.176.232.124:443`
- `159.65.88.10:8080`
- `160.16.142.56:8080`
- `216.158.226.206:443`
- `203.114.109.124:443`
- `103.43.46.182:443`
- `46.55.222.11:443`
- `209.126.98.206:8080`
- `91.207.28.33:8080`
- `1.234.2.232:8080`
- `45.118.115.99:8080`

- `206.189.28.199:8080`
- `94.23.45.86:4143`
- `158.69.222.101:443`
- `103.70.28.102:8080`
- `101.50.0.91:8080`
- `58.227.42.236:80`
- `119.193.124.41:7080`
- `107.182.225.142:8080`
- `185.157.82.211:8080`
- `45.235.8.30:8080`
- `103.132.242.26:8080`
- `1.234.21.73:7080`
- `110.232.117.186:8080`
- `209.97.163.214:443`
- `185.8.212.130:7080`
- `209.250.246.206:443`

Tria.ge:

> https://tria.ge/220428-23e5saffg3/behavioral1#report

IronNet Analytics Mapped to MITRE TTPs

	MITRE ATT&CK	
IronNet Analytic	**Tactic**	**Technique**
Consistent Beaconing HTTP/TLS	Command and Control	Application Layer Protocol
Domain Analysis HTTP/TLS	Command and Control	Application Layer Protocol

About Ironnet

Founded in 2014 by GEN (Ret.) Keith Alexander, IronNet, Inc. (NYSE: IRNT) is a global cybersecurity leader that is transforming how organizations secure their networks by delivering the first-ever Collective Defense platform operating at scale. Employing a number of former NSA cybersecurity operators with offensive and defensive cyber experience, IronNet integrates deep tradecraft knowledge into its industry-leading products to solve the most challenging cyber problems facing the world today.

Back to IronNet Blog