More_Eggs Came Calling for Easter

eSentire's security research team, the Threat Response Unit (TRU), has discovered that the stealthy more_eggs malware has re-emerged once again this year infecting corporate entities. More_eggs is malicious software containing several components engineered to steal valuable credentials, including usernames and passwords for corporate bank accounts, email accounts and IT administrator accounts, among others.

TRU has uncovered a more_eggs phishing campaign where hackers are posing as job applicants and luring Corporate Hiring Managers into downloading what they believe are resumes from job applicants. However, the bogus resumes contain the more_eggs malware.

Thus far, TRU has discovered and shut down four separate security incidents relating to the current more_eggs campaign. Three of them occurred at the end of March, and the organizations attacked include a U.S.-based aerospace/defense company; a large UK-based CPA firm; an international business law firm based out of Canada; and a national Canadian staffing agency. TRU has produced a full report outlining their findings and how best to protect against the current more_eggs threat.

Key Takeaways

- eSentire's Threat Response Unit (TRU) research team has discovered a new threat campaign using the more_eggs malware.
- More_eggs is a stealthy, lethal malware that contains components engineered to steal usernames and passwords for corporate bank accounts, email accounts and IT administrator accounts, among others.
- The current more_eggs campaign involves hackers posing as job applicants and luring Corporate Hiring Managers into downloading what they believe are resumes from job applicants. In actuality, the resumes contain the more_eggs malware.
- TRU has detected and shut down four different more_eggs security incidents recently. Three of them occurred at the end of March, and they all involve the new variant of more_eggs. The organizations attacked include a U.S.-based aerospace/defense company that designs, develops and provides maintenance repair for airline components; a large UK-based CPA firm; an international business law firm based out of Canada; and a national Canadian staffing agency.
- One year ago, TRU also discovered a spearphishing campaign infecting victims with more_eggs. However, during that operation, the threat actors were targeting professionals on LinkedIn who were looking for jobs, as opposed to Hiring Managers looking for job candidates. The hackers sent the job seekers .zip files disguised as job offers. When the targets opened the zip file, it led to the installation of more_eggs.

Research Report

A more_eggs malware campaign has appeared, just as it did last year during the Easter season. eSentire's Threat Response Unit (TRU) security research team has discovered a phishing campaign where hackers are posing as job applicants and luring Corporate Hiring Managers into downloading what they believe are resumes from job applicants. However, the bogus resumes contain the more_eggs malware.

More_eggs is a stealthy, lethal malware that has several components engineered to steal valuable credentials, such as usernames and passwords for corporate bank accounts, email accounts and IT administrator accounts, among others. Once accessed, the hackers exfiltrate data from the victim organization, spread to other computer hosts via TeamViewer, and encrypt files. The Golden Chickens group (aka Venom Spider) is believed to be the threat operators behind more_eggs. Interestingly, several top financial cybercrime groups, including the infamous FIN6 gang, Evilnum and the Cobalt Group have employed the more_eggs malware in their attack campaigns.

The Current More_Eggs Operation — a Déjà Vu of the 2021 LinkedIn Campaign?

Ironically, around the same time last year in April 2021, TRU discovered a spearphishing campaign which was infecting victims with more_eggs. However, during that campaign, rather than posing as hopeful job candidates sending a poisoned resume, the threat actors targeted professionals on LinkedIn who were looking for jobs. The hackers sent the job seekers .zip files disguised as job offers. When the targets opened the zip file, it led to the installation of more_eggs. The threat actors behind the campaign tried enticing the targets into clicking on the zip file by naming the file after the job seeker's current job title and adding "position" at the end.

For example, if the LinkedIn member's job is listed as 'Senior Account Executive——International Freight,' the malicious zip file would be titled 'Senior Account Executive —— International Freight position.' Upon opening the fake job offer, the victim unwittingly initiated the installation of more_eggs.

eSentire's TRU Disrupts Attacks Against an Aerospace/Defense Company, International Law Firm, International CPA Firm and Staffing Agency

Thus far, in the current more_eggs campaign, the eSentire TRU team has discovered and shut down four separate security incidents. Three of them occurred at the end of March, and they all involve the new variant of more_eggs. The organizations attacked include a U.S.-based aerospace/defense company that designs, develops and provides maintenance repair for airline components; a large UK-based CPA firm; an international business law firm based out of Canada; and a national Canadian staffing agency.

The threat actors behind the current more_ eggs campaign don´t appear to be randomly targeting companies. For example, the CPA firm and the staffing agency, both list a job posting on Indeed.com and LinkedIn which match the title of the resume each hiring manager received. The aerospace/defense company also had a job listed on zip Recruiter.com which matches the title of the fake resume received.

What are the Hackers After?

Since these more_eggs attacks were disrupted, the TRU team cannot know with certainty what the end game is for this operation or what threat group is behind these attacks. What we do know is that this current activity demonstrates a role-reversal from last year's more_eggs LinkedIn campaign. We also know that the more_eggs Malware-as-a-Service (MaaS) is known to be utilized by the very capable FIN6, Evilnum and Cobalt cybercriminals.

Of course, for a threat group to get a foothold into the IT environments of an aerospace/ defense company, an international law firm, an international CPA firm and a national corporate staffing agency could be very lucrative. Successfully infecting a corporate employee with the more_eggs malware could potentially enable a threat actor(s) to commit a variety of cybercrimes including deploying ransomware, stealing intellectual property, stealing credentials to corporate bank accounts, or committing business email compromise, among others.

Connection Between FIN6, Evilnum, Cobalt Group and More_Eggs

FIN6 - FIN6 is a financial cybercrime group that primarily steals payment card data and sells it on underground marketplaces. The FIN6 group first gained notoriety in 2014 for their attacks against point-of-sale (POS) machines in retail outlets and hospitality companies. Continuing their quest for credit and debit card data, they later moved on to targeting e-Commerce companies and stole their credit card data via online skimming. The FIN6 threat group has also been known to infect some of their victims with ransomware.

Interestingly, intelligence analysts with Visa reported in February2019 that at the end of 2018, FIN6 was specifically targeting numerous e-Commerce companies' payment servers and using malicious documents to infect their targets with more_eggs as the initial phase of their attack.

That activity mirrors a threat campaign that was reported separately in February 2019 by ProofPoint researchers. In these incidents, threat actors were observed attacking retail, entertainment and pharmaceutical companies' online payments systems and using malicious documents, laden with more_eggs, to target the companies' employees. The threat actors sent fake job offers to the employees, cleverly using the job title listed on their LinkedIn profiles, in their communications. The campaigns reported in February 2019 by Visa and ProofPoint could be the same operation or, they could be two separate campaigns. However, what we do know is that the targets (eCommerce companies' payment systems) and tools (more_eggs) were used in both scams.

Later in August 2019, the FIN6 operators launched another malicious campaign, and researchers believe with this operation FIN6 was actively going after multinational organizations. Similar to the February 2019 campaign launched against the retail, entertainment, and pharmaceutical companies; employees were spearphished with fake job offers. According to security researchers, to gain access to victim environments, the threat actor began by targeting handpicked employees using LinkedIn messaging and email, advertising fake jobs to lure recipients into checking into the supposed offers.

Between the end of 2018 and April 2021, there have been three distinct more_eggs LinkedIn campaigns using the same Modus Operandi. Each campaign targeted corporate employees, utilized their LinkedIn profile, and then social engineered them with bogus job offers, which lead to the more_eggs malware.

Evilnum - The Evilnum cybercrime group is best known for compromising financial technology companies, which are companies that provide stock trading platforms and tools. Their target is financial information about the targeted FINTECH companies and their customers. They target items such as spreadsheets and documents with customer lists, investments and trading operations and credentials for trading software/platforms and software.The Evilnum group is also known to spearphish employees of the companies they are targeting and enclose malicious zip files. If executed, the employees get hit with the more_eggs backdoor, along with other malware.

Cobalt Group - The Cobalt Group is also known to go after financial companies, and it has repeatedly used the more_eggs backdoor in their attacks.

The Interworkings of More_Eggs

More_eggs is a sophisticated suite of malware components. One of those components is VenomLink (a component used to trick the victim into installing TerraLoader). TerraLoader is an intermediate component used to install numerous modules designed to take malicious actions such as credential theft, lateral movement, and file encryption throughout a victim's IT network. A complete analysis of the 2020 version of more_eggs was conducted by Quo Intelligence, who broke the malware into several modules. Here is a full breakdown:

- VenomLNK is a poisoned LNK file. Windows uses LNK files to automate program execution. More_eggs uses a maliciously-written LNK file to execute TerraLoader by tricking the user into opening what they think is a document.
- TerraLoader loads the other modules from VenomLNK.
- TerraPreter provides a Meterpreter (a Metasploit attack payload) shell in memory.
- TerraStealer is an info stealing module used to exfiltrate sensitive data.
- TerraTV allows threat actors to hijack TeamViewer for lateral movement.
- TerraCrypt is a ransomware plugin for PureLocker ransomware, aka CR1 Ransomware, a lesser-known ransomware.

The social engineering method for this current more_eggs campaign consisted of disguising a zipped copy of the VenomLNK malware as a job applicant's resume. A benign PDF resume is included as well, which serves as a decoy resume, while more_eggs installs TerraLoader.

As with previous more_eggs variants observed by TRU, the malware abuses legitimate Windows processes to evade detection, alongside a decoy document to trick users. With the incident involving the accounting firm, an employee of the firm received what they thought was a candidate's resume, when in actuality the resume was the VenomLNK malware. Once VenomLNK was executed, it proceeded to execute TerraLoader so that TerraLoader could then load various information stealing and intrusion modules of the more_eggs malware suite. With this campaign however, there are two notable differences:

- As stated earlier, rather than targeting hopeful candidates looking for work, the hackers are targeting businesses looking for employees.
- In place of the previously abused Windows process, cmstp.exe — which manages network connections — more_eggs is abusing ie4uinit.exe, another Windows Process, to load its malicious plugins.

What's New with More_Eggs?

The current threat campaign utilizes several similar features TRU observed in the 2021 more_eggs LinkedIn operation including: the VenomLNK module, including a decoy document, and .lnk file, and multi-phase execution through writing and reading .txt files (which turned out to be .xml files with JavaScript contents upon inspection). The TerraLoader equivalent, however, abuses ie4uinit.exe instead of cmstsp.exe, eventually leading to the abuse of msxsl.exe as we reported in April 2021.

Observations of More_Eggs Operation from Keegan Keplinger, research and reporting lead with eSentire's Threat Response Unit (TRU) security team

"Anti-Virus(AV) is not enough to protect employees and home users from cyber threats. Because malware like more_eggs takes the so-called fileless approach to evade AV, there is no malicious executable for AV to detect. Rather, more_eggs achieves execution by passing malicious code to legitimate windows processes and letting those windows processes do the work for them."

"We tend to see threat campaigns, involving the sophisticated and versatile more_eggs malware, just a few times a year compared to some other threats. In addition to the spearphishing component, this indicates to me that threat actors, using the more_eggs service, are selective and patient."

"This year the more_eggs operation has flipped the social engineering script, targeting hiring managers with fake resumes instead of targeting jobseekers with fake job offers."

"The threat actors behind more_eggs use a scalable, spearphishing approach that weaponizes expected communications, such as resumes, that match a hiring manager´s expectations or job offers, targeting hopeful candidates, that match their current or past job titles."

Recommendations for Protecting Against More_Eggs

- Security Awareness Training for All Employees. Security Awareness training should be mandated for all company employees. The training should ensure that employees:
    - Avoid downloading and executing files from unverified sources. For example, be wary of Word and Excel documents sent from an unknown source or acquired from the Internet that prompts you to 'Enable Macros'.
    - Avoid free versions of paid software.
    - Always inspect the full URL before downloading files to ensure it matches the source (e.g., Microsoft Team should come from a Microsoft domain).
    - Inspect file extensions. Do not trust the filetype logo alone. An executable file can be disguised as a PDF or office document.
    - Ensure standard procedures are in place for employees to submit potentially malicious content for review
- Anti-virus isn't enough. Malware that abuses LOLBINs bypasses binary detection approaches. Therefore, Endpoint Detection and Response (EDR) agents need to be installed on all hosts. An EDR solution is a necessary technology for detecting threats such as more_eggs ,and EDR agents must be continuously monitored and updated with the evolving threat landscape. If not, then critical alerts will not be triaged and investigated. Managed Detection and Response (MDR) providers offer this service. Robust and comprehensive MDR services require an AI-powered Extended Detection and Response (XDR) technology platform so that the hundreds of daily security signals, generated by an organization's EDR agents, can be promptly ingested, analyzed and responded to. Security events which can be resolved through an automated response are processed, while security events requiring a hands-on response are handled by the MDR's cybersecurity analysts and threat hunters.
- Monitor the Threat Landscape. Organizations need relevant threat intelligence, and it must be actioned in a timely fashion. Additionally, one's security team needs to be specifically informed about an organization's operating environment, working in concert with one's security provider.

If you're not currently engaged with a Managed Detection and Response provider, we highly recommend you partner with us for security services to disrupt threats before they impact your business. Want to learn more about how we protect organizations globally? Connect with an eSentire Security Specialist.

Glossary

More_eggs — a malware suite that includes a social engineering initial access vector (VenomLNK), a plugin loader (TerraLoader) that loads modules, and functional modules that are capable of infostealing (TerraStealers) meterpreter shells (TerraPreter), and evasive lateral movement (TerraTV). See The Interworkings of More_Eggs section for more.

Infostealing — infostealing capabilities in malware can be geared towards a variety of information targets such as configuration options (like stealing cookies to simulate the victim's web sessions), login credentials saved in browsers and files, and credit card information (saved in browsers).

Meterpreter — meterpreter is a pentesting tool that contains a large library of exploits and intrusion tools used for different purposes including privilege escalation, credential theft, lateral movements, and both local and remote code execution.

Golden Chickens — also known as Venom Spider, Golden Chickens has been operating the more_eggs malware-as-a-service since at least 2018.

LOLBINS — stands for Living-Off-The-Land-Binaries and represents a class of Windows processes that can be abused in malware, such as more_eggs.

Privilege Escalation — when a threat actor gets higher permissions for an account they've compromised or can get access to a more powerful account.

Lateral Movement — when threat actors can compromise additional, sometimes more powerful assets (such as Exchange Servers or Domain Controllers) in the organization from their initial foothold.

Domain Controllers — A central defining infrastructure in most enterprise networks. The domain controllers help define and manage the internal network and who can access what on it.

Indicators

SHA256

0d5b74add9fd68c54d8c7df883fa727d74dacc0bff3c49afd200b914e6051d9a
822e1359b7e7eabc9199a055fd772819176d2e5cae63d0d24787579634d45d42
86680bef3d1e41f369ab60acf8198496a367fbb7183d5f1104230a74d32705b3
d6906cb7f9fb0f9cd12943509a1bb5e9409a4547a18f930b071d5c330e6c97f9 88b0b1d9988fb2a42934f862944be0b32d00cb5e6ffc71e3164fa7c4cacff62d

LOLBIN ingress:

c:/users/<username>/appdata/roaming/microsoft/msxsl.exe c:/users/<username>/appdata/roaming/microsoft/ie4uinit.exe

Account Discovery: net group /domain "Domain Admins"

Domain Discovery: nltest /trusted_domains

Joe’s Sandbox Analysis: https://www.joesandbox.com/analysis/564458/0/html

ATT&CK Tactic	ID	Name	Description
Execution	T1059.003	Windows Command Shell	More_eggs has used cmd.exe for execution.
Execution	T1059	Command and Scripting Interpreter	...
Privilege Escalation	T1546.003	Windows Management Instrumentation Event Subscription	ENT
Defense Evasion	T1027	Obfuscated Files or Information	More_eggs's payload has been encrypted with a key that has the hostname and processor family information appended to the end.
Defense Evasion	T1070.004	File Deletion	More_eggs can remove itself from a system.
Defense Evasion	T1070	Indicator Removal on Host	...
Defense Evasion	T1140	Deobfuscate/Decode Files or Information	More_eggs will decode malware components that are then dropped to the system.
Defense Evasion	T1218.010	Regsvr32	More_eggs has used regsvr32.exe to execute the malicious DLL.
Defense Evasion	T1218	Signed Binary Proxy Execution	...
Defense Evasion	T1220	XSL Script Processing	msxsl.exe was used to bypass defenses and to invoke Jscript code from an XSL file.
Defense Evasion	T1553.002	Code Signing	More_eggs has used a signed binary shellcode loader and a signed Dynamic Link Library (DLL) to create a reverse shell.
Defense Evasion	T1553	Subvert Trust Controls	..
Discovery	T1016.001	Internet Connection Discovery	More_eggs has the capability to gather the IP address from the victim's machine.
Discovery	T1016	System Network Configuration Discovery	...
Discovery	T1033	System Owner/User Discovery	More_eggs has the capability to gather the username from the victim's machine.

ATT&CK Tactic	ID	Name	Description
Discovery	T1069.002	Domain Groups	net group /domain "Domain Admins" was used to gather information about domain groups
Discovery	T1069	Permission Groups Discovery	...
Discovery	T1082	System Information Discovery	More_eggs has the capability to gather the OS version and computer name.
Discovery	T1482	Domain Trust Discovery	nltest /trusted_domains was used to gather domain trust information
Discovery	T1518.001	Security Software Discovery	More_eggs can obtain information on installed anti-malware programs.
Discovery	T1518	Software Discovery	...
Command and Control	T1071.001	Web Protocols	More_eggs uses HTTPS for C2.
Command and Control	T1071	Application Layer Protocol	...
Command and Control	T1105	Ingress Tool Transfer	More_eggs can download and launch additional payloads. (msxsl.exe was downloaded & installed)
Command and Control	T1132.001	Standard Encoding	More_eggs has used basE91 encoding, along with encryption, for C2 communication.
Command and Control	T1132	Data Encoding	...
Command and Control	T1573.001	Symmetric Cryptography	More_eggs has used an RC4-based encryption method for its C2 communications.
Command and Control	T1573	Encrypted Channel	...

Skip To: