

```
# the program decrypts a phrase

def rot13(message):
    r = ''
    for m in message:
        ab = ord(m)
        av = 0

        if ab < 110 and ab > 97:
            av = ab + 13
        elif ab > 110 and ab < 122:
            av = ab - 13
        else:
            av = ab
        ascii = chr(av)
        r = r+ascii
    return r
key = input('encrypted word: ')
print('decryption: ', rot13(key))
```

Account Creation

Include the output of whoami and sudo ls as that user

```
aggie@amata-VirtualBox:~$ sudo ls
[sudo] password for aggie:
Desktop Documents Downloads Music Pictures Public Templates Videos
aggie@amata-VirtualBox:~$ whoami
aggie
aggie@amata-VirtualBox:~$
```

Find the logs of your sudo command and include it below.

```
aggie@amata-VirtualBox:~$ sudo tail /var/log/auth.log
Sep 13 22:03:55 amata-VirtualBox dbus-daemon[1196]: [system] Failed to activate
service 'org.bluez': timed out (service_start_timeout=25000ms)
Sep 13 22:04:03 amata-VirtualBox sudo: pam_unix(sudo:auth): Couldn't open /etc/
securetty: No such file or directory
Sep 13 22:04:05 amata-VirtualBox sudo: pam_unix(sudo:auth): Couldn't open /etc/
securetty: No such file or directory
Sep 13 22:04:05 amata-VirtualBox sudo:      aggie : TTY=pts/0 ; PWD=/home/aggie ;
USER=root ; COMMAND=/usr/bin/ls
Sep 13 22:04:05 amata-VirtualBox sudo: pam_unix(sudo:session): session opened f
or user root by (uid=1003)
Sep 13 22:04:05 amata-VirtualBox sudo: pam_unix(sudo:session): session closed f
or user root
Sep 13 22:04:53 amata-VirtualBox pkexec: pam_unix(polkit-1:session): session op
ened for user root by (uid=1003)
Sep 13 22:04:53 amata-VirtualBox pkexec[6639]: aggie: Executing command [USER=r
oot] [TTY=unknown] [CWD=/home/aggie] [COMMAND=/usr/lib/update-notifier/package-
system-locked]
Sep 13 22:05:40 amata-VirtualBox sudo:      aggie : TTY=pts/0 ; PWD=/home/aggie ;
USER=root ; COMMAND=/usr/bin/tail /var/log/auth.log
Sep 13 22:05:40 amata-VirtualBox sudo: pam_unix(sudo:session): session opened f
or user root by (uid=1003)
```

Bob and Betty

Create a new file by bob, include the ls of the file and show that betty can read the file

```
betty@amata-VirtualBox:~$ ls -al /data/newgroup
total 8
drwxrwsr-x 2 root  newgroup 4096 Sep 14 17:06 .
drwxr-xr-x 3 root  root    4096 Sep 14 16:53 ..
-rw-rw-r-- 1 betty newgroup  0 Sep 14 17:06 newfile
betty@amata-VirtualBox:~$
```

Include a screenshot of betty running nmap and failing at other commands using sudo

```

betty@amata-VirtualBox:~$ sudo /usr/bin/nmap
Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sV/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<|ipt kiddi3,
    and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
betty@amata-VirtualBox:~$

```

```

betty@amata-VirtualBox:~$ sudo ls
[sudo] password for betty:
Sorry, user betty is not allowed to execute '/usr/bin/ls' as root on amata-VirtualBox.
betty@amata-VirtualBox:~$

```

The Magento (an e-commerce platform written in PHP) has recently undergone web injection. Fortunately, the threat intelligence analyst team was able to catch malicious attacks from the new credit card malware running Magento 1. The analysts probably used some data analysis techniques to identify patterns and trends within datasets. The article says that a similar attack had already happened in 2020 that leveraged another skimmer and negatively impacted 3,000 domains. The new malware is disguised as a favicon and is called Magento.png. It targets websites via PHP web shell. This type of attack is called Magecart and is used with JavaScript-based web injections on Magento websites. The purpose of this attack is to obtain customers' card information. The article explains that if the attackers could have used JavaScript instead of PHP, it would trigger the system, but since they targeted PHP, it didn't work the same way. The team says that online sellers have to keep their stores "up-to-date and hardened." The article does not explicitly state how this could have been prevented, but my guess is that such an attack could easily be overlooked by the human eye because this involves scripts. Therefore, the data security team could've checked their scripts and system weekly to ensure that their data has not been compromised.

<https://portswigger.net/daily-swig/magecart-group-12-unleashes-stealthy-php-skimmer-against-vulnerable-magento-e-commerce-sites>

For these three, I used tshark and filtered the results. Pcap1.pcap and pcap2.pcap displayed windows, lengths, and acknowledgments signifying something were blocking the signal and an acknowledgment was needed to pass it. Pcap1.pcap contained several malformed packets. Most of the packets came from a web server via HTTP, indicating that something was being browsed.

Pcap2.pcap also included some connections to the website via DNS when a person visited a government weather website that broadcast traffic. Other searches involved Miami, too. In some cases, pcap2.pcap and pcap3.pcap showed that Windows's sound driver was involved with broadcast traffic.

At one point, Pcap3.pcap showed an upload to Wikimedia.org and a download of images from Wikipedia using DNS and HTTP. In addition, the person probably encountered an unreachable destination at some point, which means that something was blocking them from accessing it, like a firewall.

By applying tcpextract to all of these, I found two pictures (a poster and a cake), a bunch of fcs videos I couldn't open, and html pages with Java code about weather and media.

1. Use John to crack your /etc/shadow in your VM. Include the output below. Let John run for a max of 1 hour. Do not include any sensitive passwords, if they are throw away passwords (like aggie) then leave them in.

```
root@amata-VirtualBox:/home/amata# john /etc/shadow
Loaded 3 password hashes with 3 different salts (crypt)
Warning: OpenMP is disabled; a non-OpenMP build may be slower
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:07 56% 1/3 0g/s 528.0p/s 528.0c/s 528.0C/s
0g 0:00:00:09 64% 1/3 0g/s 526.8p/s 526.8c/s 526.8C/s
0g 0:00:00:13 85% 1/3 0g/s 525.6p/s 525.6c/s 525.6C/s
123456
0g 0:00:00:16 98% 1/3 0g/s 521.0p/s 521.0c/s 521.0C/s
915
123 (aggie)
```

2. Use Hydra to crack the Login page. Include the command you ran and the cracked password

```
amata@amata-VirtualBox:~/pyflask/pyflask$ hydra -l admin -P 10-million-password
-list-top-1000000.txt 127.0.0.1 -s 5000 http-post-form "/login:username=^USER^&
password=^PASS^:F=Error"
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in m
ilitary or secret service organizations, or for illegal purposes (this is non-b
inding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-11-18 12:45
:09
[DATA] max 16 tasks per 1 server, overall 16 tasks, 999998 login tries (l:1/p:9
99998), ~62500 tries per task
[DATA] attacking http-post-form://127.0.0.1:5000/login:username=^USER^&password
=^PASS^:F=Error
[5000][http-post-form] host: 127.0.0.1 login: admin password: admin
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 7 final worker threads did not complete
until end.
[ERROR] 7 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-11-18 12:45
:24
```

When I ran the analysis on my network, it didn't find any vulnerabilities. But it did find multiple ports that my host's using.

I looked up at the library and helpdesk hosts. It didn't find any vulnerabilities. When I opened the port analysis, it gave me plugin details. Both plugins were published in the 2005 year and were modified in September 2021, which probably means that the websites are maintained, updated, and properly secured every year. Based on the library's information about the ping remote host, the library's network uses an ICMP echo packet instead of an actual port. While the helpdesk's remote host replied to a TCP SYN packet sent to port 80 with a SYNACK packet. I ran another analysis for other USU networks but didn't find anything particularly interesting.

Since I don't usually get suspicious/fishing emails (which is good, I guess), I picked the spam from my phone instead of my email. I received a link to a website sent to my old phone with a domain name patriciaterry.club. It was sent to me as a message on my phone, but the contact name is a Gmail email address. I performed vlookup via Talos. It was unable to identify the sender's location, and its reputation was rated as neutral.

When I added it to VirusTotal, Fortinet labeled it as spam, while others showed it clean.

When I run a whois command on my VM, most of the personal information is hidden.

The registrant country is Iceland (Capital Region), it's registered on Namecheap company, the creation year is 2021, and the expiration year is 2022. The status of the domain is active. The domain's traffic provided me with a non-authoritative answer from Amazon. The source didn't have much to capture, but I did find an index page that leads to some Domain website. I suspect this type of attack was smishing, as the attacker was trying to obtain personal information from me.

<https://threatpost.com/ikea-email-reply-chain-attack/176625/>

Key factors:

- IKEA phishing internal emails to employees.
- The Phishing emails contain links ending in seven digits and may include attachments with Microsoft Office documents (example: Excel) or links to cloud storage that is infected with the QakBot malware.

Other corporations, including Cisco, were affected by similar attacks. The attackers use the same tactics; they target masses, leaving signs behind.

- QakBot with the ProLock work by launching PowerShell and may also gain access to cloud storage, encrypting the victim's files, then asking for payment to decrypt them. Assumption: there's a distinct group of hackers who target corporations. Their motivation is money.
- Hijacking email replies is one technique to avoid spam suspicions and getting flagged/quarantined by email gateways.
- Attackers exploit ProxyLogon and ProxyShell vulnerabilities.
- Temporary solution: the IT department disabled the release of all quarantined emails.


Proposal

In an abundance of caution, new emails will be created which will be aligned with the employee's unique identifier and password. The old emails will be disabled and removed within four days. We recommend setting up multi-factor authentication using two different applications on your phone after receiving a new email. The applications will be protected by additional login credentials and biometric authentication. Employees who do not possess a phone capable of supporting the following features will be provided with a new one. Sending messages containing attachments or links will now require verification through a randomized code provided by the MFA app used for login to the new email.

The anti-phishing and safe links policies will also be implemented. These policies include enabling machine learning models to recognize sensitive data, classifying sensitive data, applying TLS based encryption to message transmission, scanning the reputation of links, and using ATP Safe Attachment for Microsoft Office documents.




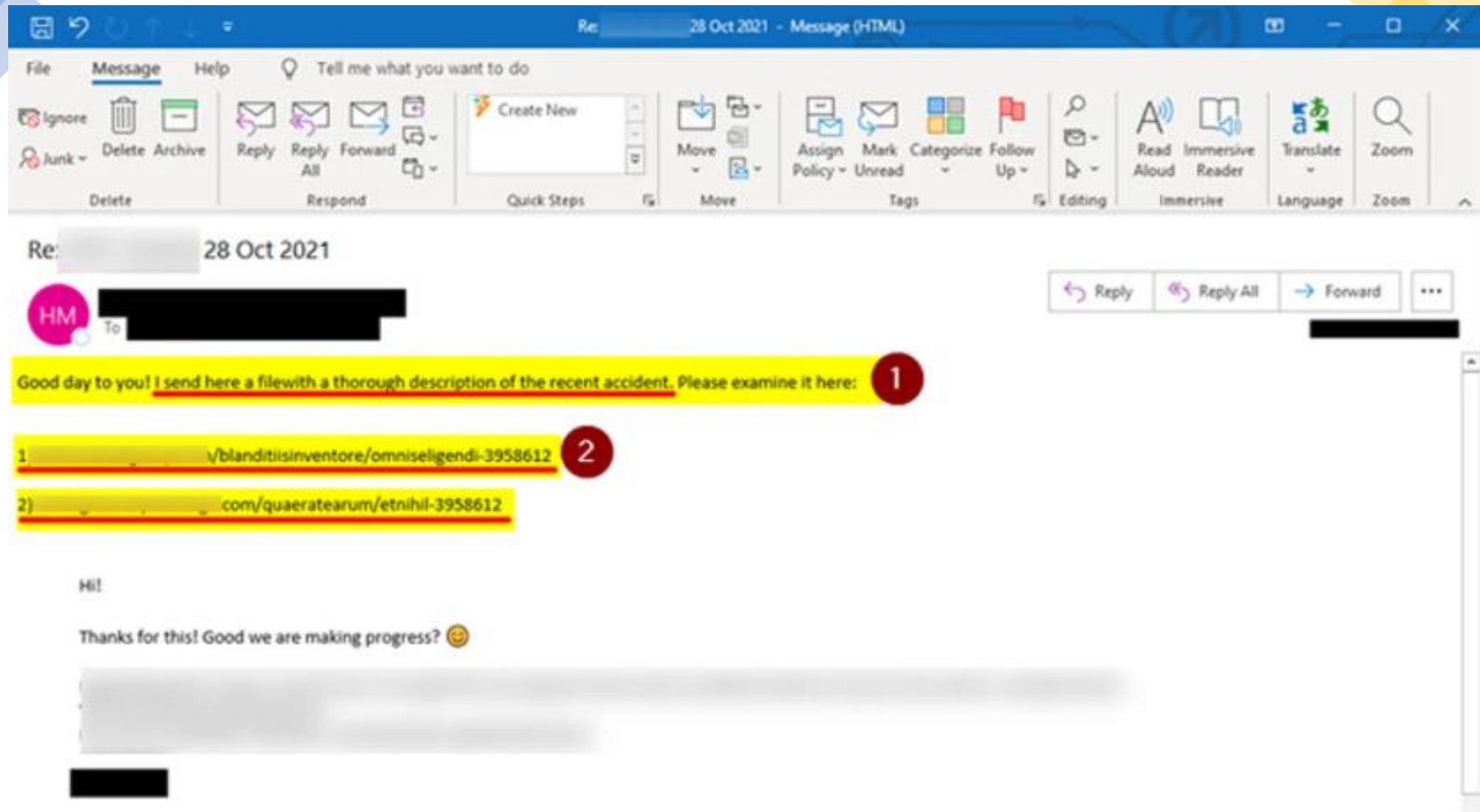
IKEA hit by Email Reply- Chain Cyberattack



"There is an ongoing cyberattack that is targeting Inter IKEA mailboxes. Other IKEA organisations, suppliers, and business partners are compromised by the same attack and are further spreading malicious emails to persons in Inter IKEA.

"This means that the attack can come via email from someone that you work with, from any external organisation, and as reply to an already ongoing conversation. It is therefore difficult to detect, for which we ask you to be extra cautious." –IKEA internal email to employees.



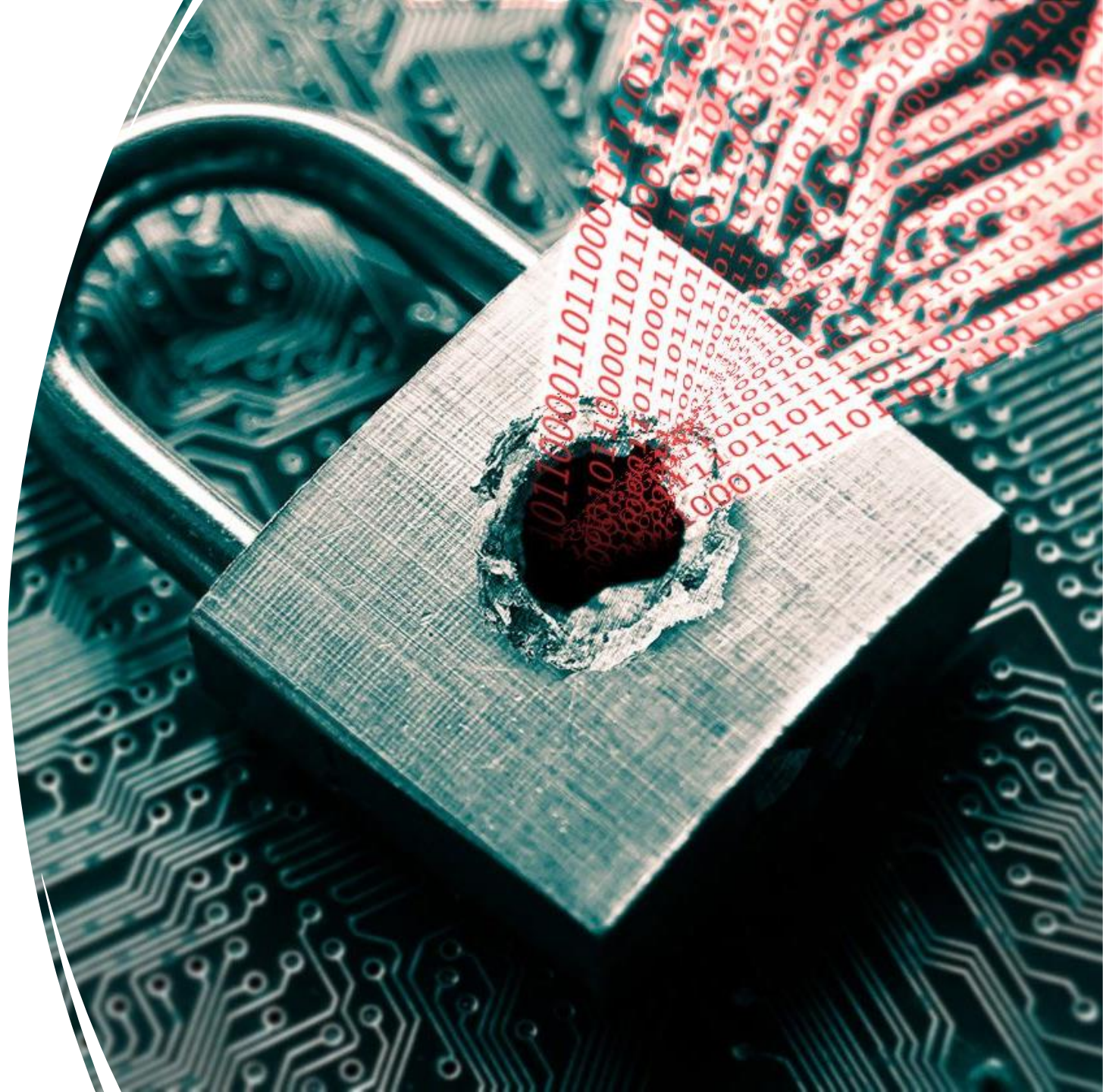


Example phishing email sent to IKEA employees

Squirrelwaffle, ProxyShell, and ProxyLogon

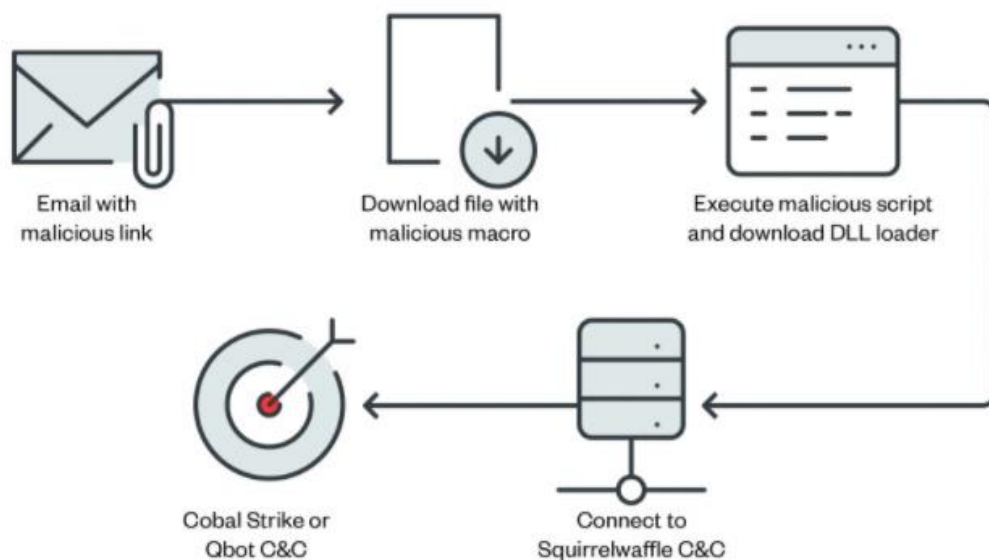
Squirrelwaffle is a malicious software usually delivered using spam email campaigns.

ProxyShell and **ProxyLogon** are vulnerabilities on Microsoft Exchange servers and enable remote code execution.

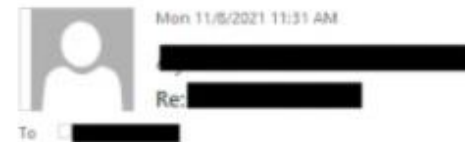




Here is an example of a hijacked email chain process



©2021 TREND MICRO



Greeting! Our specialists composed desired document and I send it to you. Document can be found through this link:

1)aayomsolutions.co.in/etiste/quasnam-4966787

2)aparnashealthfoundation.aayom.com/quasisuscipit/totamet-4966787



Proposal

- New emails (employee's unique identifier and password)
- The old emails needs to be disabled and removed
- Setting up multi-factor authentication using two different applications
- Sending attachments or links will require verification (MFA)

New anti-phishing and safe links policies

- Machine learning models
- Classifying sensitive data
- TLS based encryption
- Link reputation scan
- ATP Safe Attachment

Sources:

<https://threatpost.com/ikea-email-reply-chain-attack/176625/>

<https://threatpost.com/squirrelwaffle-loader-malspams-packing-qakbot-cobalt-strike/175775/>

<https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/safe-attachments?view=o365-worldwide>