

Relatório Operacional de CTI (Cyber Threat Intelligence)

A empresa Good Money Financial sofreu um incidente de segurança envolvendo a suspeita de comprometimento de um servidor e possível vazamento de informações sensíveis de clientes. Como parte da resposta ao incidente, foi analisado um PCAP de um computador afetado utilizando a ferramenta Zeek, com foco na identificação de Indicadores de Comprometimento (IoCs).

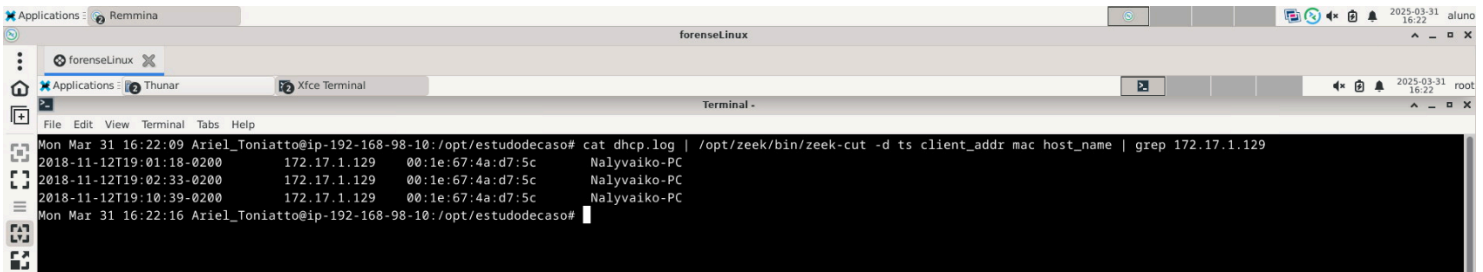
Analista Responsável: Ariel Toniatto

Resumo das Descobertas

A análise do tráfego de rede (PCAP) utilizando as ferramentas **Zeek**, **VirusTotal** e **Hybdril Analysis** revelou atividades maliciosas associadas ao host de IP **172.17.1.129**, onde inicialmente foi encontrado um **trojan downloader** que progrediu a infecção para **trojan banqueiro (Emotet)**.

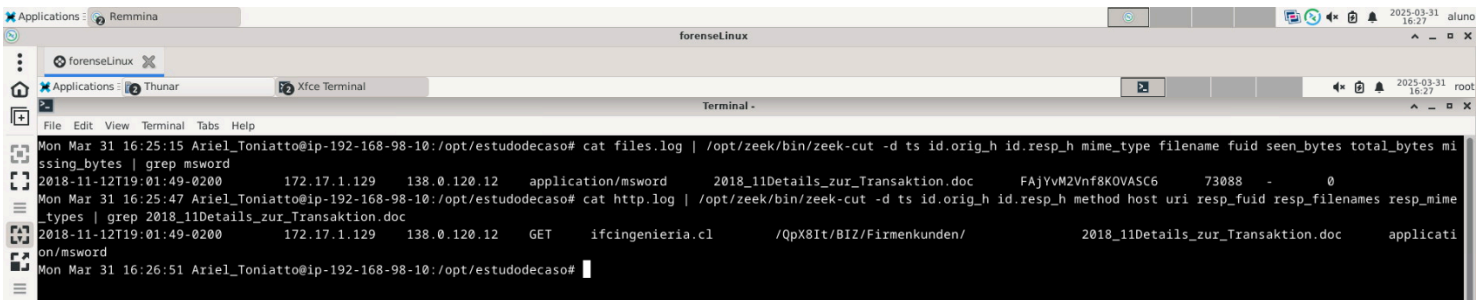
Principais descobertas:

1. **Dados do host:** O host foi identificado pelo endereço MAC: **00:1e:67:4a:d7:5c** e com o nome do host do cliente Windows **Nalyvaiko-PC**.



```
Mon Mar 31 16:22:09 Ariel_Toniatto@ip-192-168-98-10:/opt/estudodecaso# cat dhcp.log | /opt/zeek/bin/zeek-cut -d ts client_addr mac host_name | grep 172.17.1.129
2018-11-12T19:01:18-0200 172.17.1.129 00:1e:67:4a:d7:5c Nalyvaiko-PC
2018-11-12T19:02:33-0200 172.17.1.129 00:1e:67:4a:d7:5c Nalyvaiko-PC
2018-11-12T19:10:39-0200 172.17.1.129 00:1e:67:4a:d7:5c Nalyvaiko-PC
Mon Mar 31 16:22:16 Ariel_Toniatto@ip-192-168-98-10:/opt/estudodecaso#
```

2. **Download de Documento Malicioso:** O arquivo **2018_11Details_zur_Transaktion.doc** foi baixado da URL suspeita **ifcingenieria.cl/QpX8It/BIZ/Firmenkunden/**, identificada como maliciosa no VirusTotal (score 7/94) e no Hybrid Analysis, classificando o arquivo como **Trojan Downloader**.



```
Mon Mar 31 16:25:15 Ariel_Toniatto@ip-192-168-98-10:/opt/estudodecaso# cat files.log | /opt/zeek/bin/zeek-cut -d ts id.orig_h id.resp_h mime_type filename fuid seen_bytes total_bytes mime_type | grep msword
2018-11-12T19:01:49-0200 172.17.1.129 138.0.120.12 application/msword 2018_11Details_zur_Transaktion.doc FAjYvM2Vnf8KOVASC6 73088 - 0
Mon Mar 31 16:25:47 Ariel_Toniatto@ip-192-168-98-10:/opt/estudodecaso# cat http.log | /opt/zeek/bin/zeek-cut -d ts id.orig_h id.resp_h method host uri resp_fuid resp_filenames resp_mime_types | grep 2018_11Details_zur_Transaktion.doc
2018-11-12T19:01:49-0200 172.17.1.129 138.0.120.12 GET ifcingenieria.cl /QpX8It/BIZ/Firmenkunden/ 2018_11Details_zur_Transaktion.doc applicati
on/msword
Mon Mar 31 16:26:51 Ariel_Toniatto@ip-192-168-98-10:/opt/estudodecaso#
```

← → ↻ https://www.hybrid-analysis.com/sample/09ebe4229a74cdb1212671e6391742cc6bee387bf14da02974b07857b27f9223/66e6230f11cf851bb8040339

HYBRID ANALYSIS Sandbox Quick Scans File Collections Resources Request Info

🔍 IP, Domain, Hash...

2018_11Details_zur_Transaktion.doc

This report is generated from a file or URL submitted to this webservice on September 14th 2024 23:58:08 (UTC)
Guest System: Windows 11 64 bit, Professional, 10.0 (build 22621), Office 2010 v14.0.6
Report generated by **Falcon Sandbox** © Hybrid Analysis

Overview Sample unavailable Downloads External Reports Re-analyze Hash Not Seen Before No similar samples Report False-Positive Request Report Deletion

malicious
Threat Score: 100/100
AV Detection: 89%
Labeled as: Trojan.Generic
#malicious #macros-on-open

X Post Link E-Mail

09ebe4229a74cdb1212671e6391742cc6bee387bf14da02974b07857b27f9223

49 / 63
Community Score

49/63 security vendors flagged this file as malicious

09ebe4229a74cdb1212671e6391742cc6bee387bf14da02974b07857b27f9223
HTTP-FAJYvMZvNf8KOVASC6.doc
Size: 71.38 KB | Last Analysis Date: 1 day ago

doc auto-open macros long-sleeps detect-debug-environment macro-run-file run-file calls-wmi

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 9

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Code insights

The macro defines two functions: "AWQcovL" and "Document_open".
The "AWQcovL" function initially sets a constant variable "LdoDBUI" to 0. It then proceeds through a series of "if" statements that follow a pattern: checking if a variable is not 0 or a corresponding boolean.
[Show more](#)

Crowdsourced AI

Hispasser flags this file as malicious
The provided macro code exhibits several characteristics commonly associated with malicious behavior.
[Show more](#)

Popular threat label: downloader.w97m/bbfldlr Threat categories: downloader trojan Family labels: w97m obfldlr heur2

3. **Segunda Etapa de Infecção (Emotet):** O malware realizou o download do arquivo **6169583.exe** através da URL **timlinger.com/nmw/** com IP **216.37.42.32**, confirmado como **Trojan Emotet** (Trojan Banqueiro) pelo **VirusTotal** e **Hybrid Analysis**.

69e731afb5f27668b3a77e19a15e62cce84e623404077a8563fc61450d8b741

61 / 69
Community Score

61/69 security vendors flagged this file as malicious

69e731afb5f27668b3a77e19a15e62cce84e623404077a8563fc61450d8b741
CEUTIL.DLL
Size: 419.00 KB | Last Analysis Date: 25 days ago

peexe checks-user-input direct-cpu-clock-access spreader detect-debug-environment


DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 4

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.emotet/dirg Threat categories: trojan banker Family labels: emotet dirg

← → ↻ https://www.hybrid-analysis.com/sample/69e731afb5f27668b3a77e19a15e62cce84e623404077a8563fcf61450d8b741/67ed043870c9dca358075230 ☆

HYBRID ANALYSIS Sandbox Quick Scans File Collections Resources Request Info

nmw(1) 

This report is generated from a file or URL submitted to this webservice on April 2nd 2025 09:32:41 (UTC)
Guest System: Windows 11 64 bit, Professional, 10.0 (build 22621),
Report generated by **Falcon Sandbox** © Hybrid Analysis

Threat Score: 100/100
AV Detection: 90%
Labeled as: Trojan.Emotet
#windows-server-utility

Overview Sample unavailable Downloads External Reports Re-analyze Hash Seen Before No similar samples Report False-Positive Request Report Deletion

Post Link E-Mail

4. **Possível propagação de phishing:** Através da análise do seu comportamento, foi identificado um aumento de 11 e-mails enviados (antes: 0) após a sua identificação, sugerindo tentativas de phishing pelo malware.

Indicadores de Comprometimento (IoCs)

IPS:

- **IP do Host Infectado:**
 - 172.17.1.129 (Nalyvaiko-PC).
- **IPs Maliciosos:**
 - 138.0.120.12 (servidor do arquivo 2018_11Details_zur_Transaktion.doc).
 - 216.37.42.32 (servidor do arquivo 6169583.exe).
- **URLs:**
 - http://ifcingenieria.cl/OpX8It/BIZ/Firmenkunden/2018_11Details_zur_Transaktion.doc (origem do documento malicioso).
 - <http://timlinger.com/nmw/> (origem do malware Emotet).
- **Arquivos:**
 - 2018_11Details_zur_Transaktion.doc (Microsoft Word).
 - **Hashes**
 - **MD5:** 5d0dd6d7035f30516e5514928c315dc1
 - **SHA256:** 09ebe4229a74cdb1212671e6391742cc6bee387bf14da02974b07857b27f9223
 - 6169583.exe (executável).
 - **Hashes**
 - **MD5:** dd3caeac240dd38b90c015be52883a6f
 - **SHA256:** 69e731afb5f27668b3a77e19a15e62cce84e623404077a8563fcf61450d8b741

Recomendações

1. Isolamento do Host Infectado

- 1.1. Desconectar **Nalyvaiko-PC** da rede para evitar propagação.
- 1.2. Realizar análise forense para a remoção de artefatos residuais.

2. Bloqueio de IoCs na Infraestrutura

- 2.1. Adicionar a blacklist os IPs e URLs dos servidores de host, bem como os associados a eles encontrados nas plataformas Virus Total e Hybrid Analysis.

- 2.2. Atualizar regras de Firewalls e IPs para bloquear tráfego associado.
3. **Medidas Preventivas Adicionais (Conforme o CTIR Gov)**
- 3.1. Gestão de Vulnerabilidades:
- 3.1.1. Priorizar correção de vulnerabilidades antigas (ex.: CVE associadas a macros maliciosas).
- 3.1.2. Implementar política de atualizações automáticas de sistemas e aplicativos.
- 3.2. Bloqueio de Macros:
- 3.2.1. Desativar macros em documentos Office por padrão, especialmente em arquivos recebidos externamente.
- 3.3. Política de Privilégios Mínimos:
- 3.3.1. Restringir direitos administrativos e implementar Gestão de Acesso Privilegiado (PAM).
- 3.4. Listas de Reputação:
- 3.4.1. Utilizar listas de IPs/URLs maliciosas em ferramentas de segurança (ex.: proxies, firewalls).
- 3.5. Implementar soluções de detecção de atividades suspeitas (ex.: tráfego C2, acesso a domínios maliciosos).
- 3.6. Treinamento de Conscientização:
- 3.6.1. Educar usuários e colaboradores sobre phishing e riscos de anexos desconhecidos.
- 3.7. Resposta a Incidentes:
- 3.7.1. Notificar a equipe de SOC/NOC e revisar backups críticos.

Referências

- **Zeek:**
 - <https://www.zeek.org/>
- **Kaspersky Emotet:**
 - <https://www.kaspersky.com.br/resource-center/threats/emotet>
- **CTIR Gov: Medidas contra Emotet e Trickbot:**
 - <https://www.gov.br/ctir/pt-br/assuntos/noticias/2023/ameaca-cibernetica-ativa-emotet-e-trickbot>
- **VirusTotal:**
 - <https://www.virustotal.com/>
- **Hybrid Analysis:**
 - <https://www.hybrid-analysis.com/>