BOLETIM DE SEGURANÇA

Novo kit de phishing tem como alvo contas Microsoft 365 e Gmail

heimdall
security research
A DIVISION OF ISH

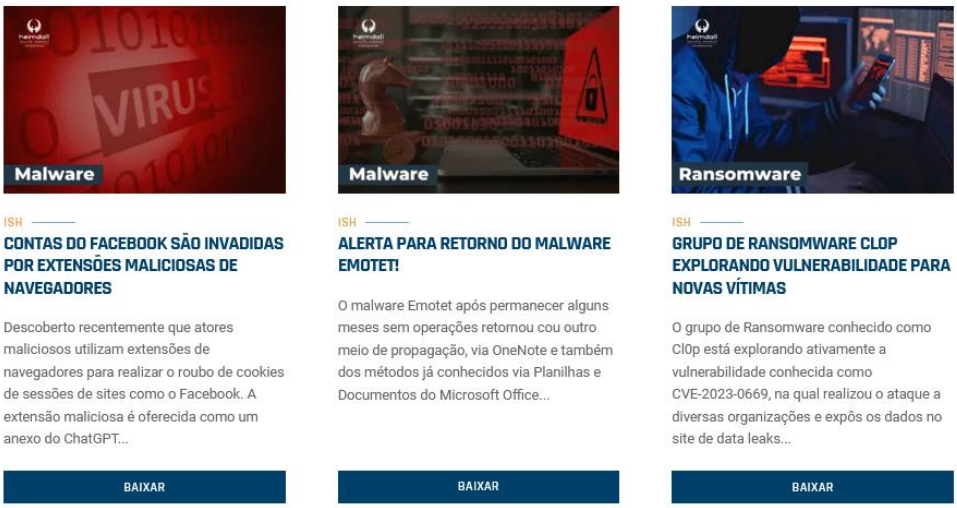
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

[Heimdall Security Research]

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

[Boletins de Segurança – Heimdall]



SUMÁRIO

LISTA DE TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Em outubro de 2023, a equipe Sekoia, identificou uma nova plataforma de *phishing-as-a-service* (**PhaaS**), denominada '**Tycoon 2FA**'. Esta plataforma foi projetada para atacar contas do Microsoft 365 e Gmail, burlando a proteção da autenticação de dois fatores (**2FA**). No entanto, em fevereiro de 2024, uma versão atualizada do Tycoon 2FA começou a circular amplamente. Esta versão atualizada apresenta melhorias significativas em seus recursos de ofuscação e anti-detecção, além de alterar os padrões de tráfego de rede.

2 DETALHES SOBRE A OPERAÇÃO

Foi identificado um aumento no uso de códigos QR em campanhas de phishing, redirecionando para diversos kits de phishing AiTM. Alguns desses kits, como **Caffeine**, **Dadsec**, **EvilProxy** e **NakedPages**, já eram monitorados, mas outros eram novos. A investigação dessas novas páginas de phishing revelou uma infraestrutura em expansão de centenas de páginas de phishing AiTM com características semelhantes.

Essas características incluíam:

- Uma página HTML compacta que continha um script que desofuscava e executava um script adicional usando operações base64 e XOR;
- Solicitações para o mesmo código JavaScript ofuscado, chamado “myscr[0-9]{6}.js”;
- Uso de uma página personalizada do CloudFlare Turnstile, uma alternativa ao CAPTCHA do Cloudflare, para proteger a página de phishing;
- Solicitações para recursos específicos de Cascading Style Sheets (CSS), chamados “pages-godaddy.css” e “pages-okta.css”;
- Uso de WebSocket para exfiltrar os dados inseridos pelo usuário.

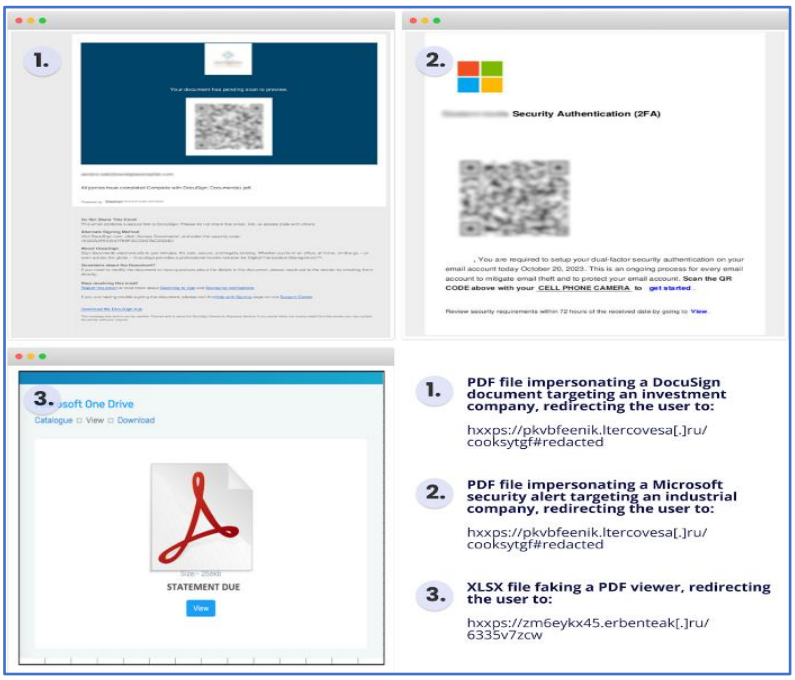


Figura 1 – E-mail redirecionando para páginas de phishing Tycoon 2FA.

Utilizando urlscan.io, foi identificado centenas de páginas de phishing em um cluster previamente desconhecido, sendo baseado nas semelhanças entre elas. Em outubro de 2023, foi divulgado uma consulta urlscan.io para localizar páginas de phishing similares, usando nomes específicos de arquivos de recursos:

filename:(“pages-godaddy.css” AND “pages-okta.css”)

As páginas de phishing mais antigas identificadas por essa abordagem buscaram seus recursos no domínio “codecrafterspro[.]com”, que aparentava ser o servidor principal desse cluster. Com o auxílio de registros DNS, registradores e WHOIS, apontou-se nomes de domínio que foi identificado como sendo do mesmo ator de ameaça.

Nome de domínio	Visto pela primeira vez
tycoongroup[.]ws	2023-07-29
codecrafters[.]su	2023-08-09
codecrafterspro[.]com	2023-08-17
devcraftingsolutions[.]com	2023-09-07

Tabela 1 – Domínios e datas associados a ameaça.

Em outubro de 2023, os domínios "**codecrafters[.]su**" e "**devcraftingsolutions[.]com**" serviam como hospedeiros para as páginas de phishing que estávamos investigando. Ambos os domínios apresentavam o mesmo painel de login, identificado como "Powered by TycoonGroup". Isso confirmou que o domínio "**tycoongroup[.]ws**" fazia parte da mesma infraestrutura. Naquele momento, o domínio estava hospedando um site que anunciava o Tycoon como a "melhor plataforma de phishing para burlar 2FA". Com base nessa evidência concreta, foi possível vincular essa infraestrutura em expansão, composta por centenas de páginas de phishing, à plataforma de phishing Tycoon 2FA.

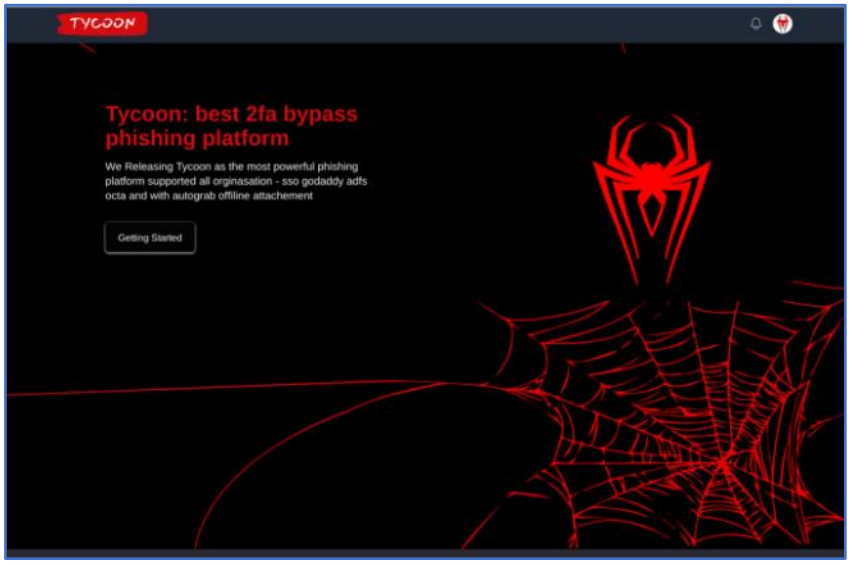


Figura 2 – Site do Tycoon 2FA.

A investigação é focada principalmente nas interações direcionadas à vítima. Não se tem acesso ao código-fonte do kit de phishing Tycoon 2FA, o que impede de analisar o back-end da infraestrutura do adversário.

O kit de phishing utiliza a técnica AiTM e envolve um servidor invasor (ou servidor proxy reverso) que hospeda a página de phishing, intercepta as entradas das vítimas, as retransmite para o serviço legítimo e solicita a autenticação MFA. Após a conclusão bem-sucedida do desafio MFA pelo usuário, o servidor intermediário captura os cookies de sessão. Esses cookies roubados permitem

que os invasores repliquem uma sessão, ignorando assim o MFA, mesmo que as credenciais tenham sido alteradas.

Abaixo, apresentamos uma visão geral detalhada das principais operações do kit de phishing Tycoon 2FA:

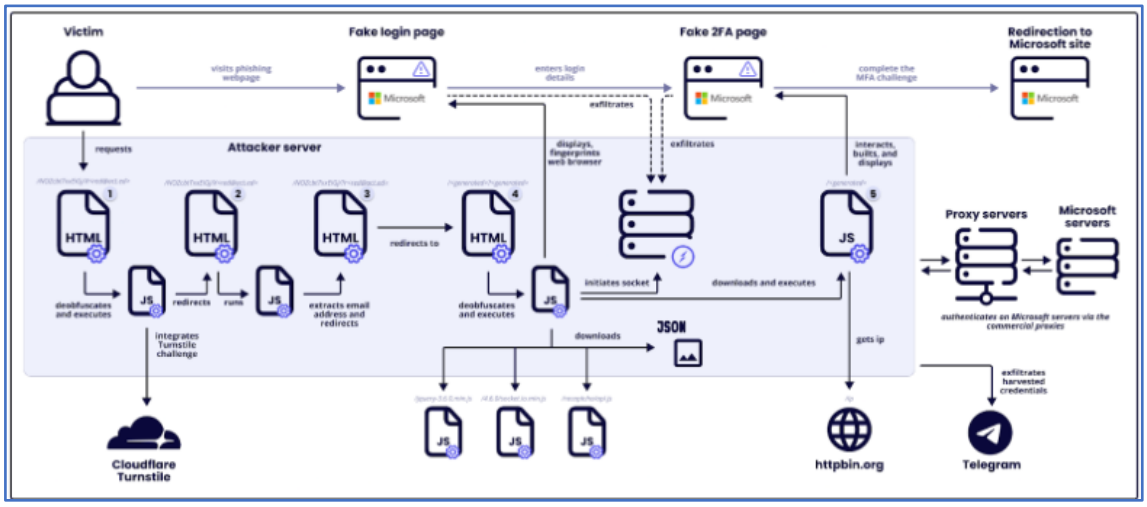


Figura 3 – Visão geral do kit de phishing Tycoon 2FA.

Os ataques são descritos em etapas distintas em que inicialmente, os atacantes disseminam links mal-intencionados através de e-mails contendo URLs ou códigos QR, induzindo as vítimas a acessarem sites de phishing, em seguida, um desafio de segurança (Cloudflare Turnstile) é usado para filtrar bots, permitindo apenas interações humanas no site de phishing, scripts ocultos são então utilizados para extrair o e-mail da vítima da URL, personalizando o ataque de phishing. Os usuários são redirecionados discretamente para outra seção do site de phishing, que os leva a uma página de login falsa. Esta página de login falsa, que se parece com a da Microsoft, é usada para roubar credenciais. WebSockets são utilizados para a exfiltração de dados. O kit de phishing simula um desafio 2FA, interceptando o token 2FA ou resposta para burlar as medidas de segurança. Por fim, as vítimas são redirecionadas para uma página que parece legítima, ocultando o sucesso do ataque de phishing.

3 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

Use métodos fortes de autenticação

- A entrada máxima da senha evita que os cibercriminosos invadam e acessem dados confidenciais. Usar um fator duas vezes (por exemplo, usar duas senhas separadas) não é considerado autenticação multifator.

Tokens de hardware

- As empresas podem fornecer tokens de hardware a seus funcionários na forma de um chaveiro que produz códigos a cada poucos segundos a um minuto.

Notificações por push

- Esse tipo de 2FA envia um sinal ao seu telefone para aprovar/negar ou aceitar/recusar o acesso a um site ou aplicativo para verificar sua identidade.

Verificação por SMS

- SMS, ou mensagens de texto, podem ser usadas como uma forma de autenticação de dois fatores quando uma mensagem é enviada para um número de telefone confiável.

Autenticação baseada em voz

- A autenticação por voz funciona de forma semelhante às notificações por push, com a diferença de que sua identidade é confirmada através da automação.

4 INDICADORES DE COMPROMISSOS

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
Domínio	0q5e0.nemen9[.]com, 25rw2.canweal[.]com, 35fu2.ouchar[.]ru, 4343w.jgu0[.]com, 43rw98nop8.m1p8z[.]com, 4m2swl.7e2r[.]com, 5me78.methw[.]ru, 6j312.rchan0[.]com, 77p3e.rimesh3[.]com, 8000n.uqin[.]ru, 8uecv.gnornamb[.]com, 98q5e.ructin[.]com, 9c43r.theq0[.]com, 9oc0y2isa27.demur3[.]com, farol. diremsto[.]com, bloggcenter[.]com, buneji.fiernmar[.]com, e85t8.nechsha[.]com, ex1uo.rhknt[.]ru, explore.atlester[.]ru, fiq75d.rexj[.]ru, fisaca.trodeckh[.]com, galume.aricente[.]com, gz238.uatimin[.]com, horizonte.sologerg[.]com, jp1y36.it2ua[.]com, k348d.venti71[.]com, kjlvo.ningeona[.]com, kjsdflwe.nitertym[.] ru, l846d.ferver8[.]com, libudi.oreversa[.]com, n29k4.ilert[.]ru n9zph.lw8opi[.]com, o6t94g.3tdx2r[.]com, oo99v.coqqwx[.]ru, p1v12.17nor[.]com, pmd8ot6xhw.3qjpc[.]com, q908q.refec7[.]com, r298y.sem01[.]com, rlpq.tk9u[.]com, roriku.orankfix[.]com, tlger-surveillance[.]com, tnyr.moporins[.]com, wasogo .shantowd[.]com, x12y.restrice[.]ru, xrs.chenebystie[.]com, xva.tjlpkcia[.]com, zaqaxu.dthiterp[.]ru, zekal6.tnjxb[.]com, zemj4f.ymarir[.]ru

Tabela 2 – Indicadores de Compromissos de Rede.

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Sekoia**
- **Bleepingcomputer**

heimdall
security research
A DIVISION OF ISH