BOLETIM DE SEGURANÇA

Malware COOKBOX sendo entregue através de vulnerabilidade WinRAR explorada pelo FlyingYeti

heimdall
security research
A DIVISION OF ISH

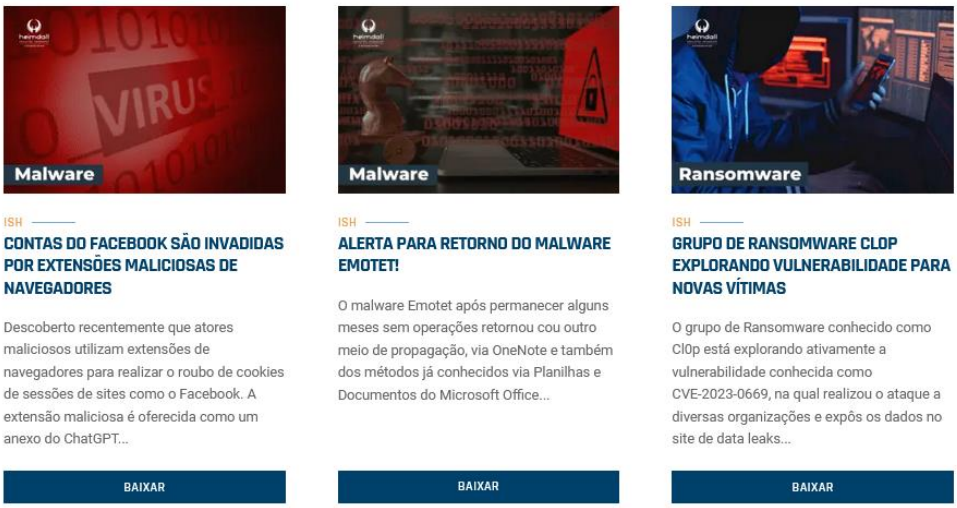
TLP: CLEAR

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

A Cloudforce One divulgou recentemente um relatório de segurança sobre a campanha de phishing associada ao ator de ameaças FlyingYeti, ligado à Rússia, que tinha como alvo de suas operações a Ucrânia, porém podendo visar outros países.

2 INFORMAÇÕES SOBRE A AMEAÇA

O FlyingYeti, é o grupo de ameaças responsável por uma campanha de phishing. Esta campanha coincide com a atividade UAC-0149, monitorada pelo CERT-UA entre fevereiro e abril de 2024. O grupo utiliza DNS dinâmico (DDNS) para estruturar sua infraestrutura e se beneficia de plataformas baseadas em nuvem para hospedar conteúdo malicioso e para comando e controle de malware (C2). Através de nossa análise dos TTPs do FlyingYeti, inferimos que o grupo provavelmente tem alinhamento com a Rússia. O foco principal do ator parece ser o ataque a entidades militares ucranianas. No código utilizado pelos atores, foi possível identificar comentários em russo no código do FlyingYeti e que o horário de operação do ator coincide com o fuso horário UTC+3.

A campanha de phishing, que foi interrompida, direcionava os alvos do FlyingYeti para uma página do GitHub sob controle dos atores em hxxps[:]//komunalka[.]github[.]io. Esta página é uma imitação do site Kyiv Komunalka (https://www.komunalka.ua), um processador de pagamentos para residentes de Kiev, permitindo o pagamento de serviços públicos e outras taxas, além de doações para as forças de defesa ucranianas. A partir de operações anteriores do ator, sabe-se que os alvos podem ser levados à página do Github do ator através de um link em um e-mail de phishing ou de uma mensagem criptografada do Signal. Ao acessar a plataforma Komunalka falsificada em hxxps[:]//komunalka[.]github[.]io, o alvo se depara com um grande botão verde que solicita o download do documento “Рахунок.docx” (“Invoice.docx. Este botão se passa por um link para uma fatura de pagamento vencida, mas na realidade leva ao download do arquivo malicioso “Заборгованість по ЖКП.rar” (“Dívida por habitação e serviços de utilidade pública.rar”).

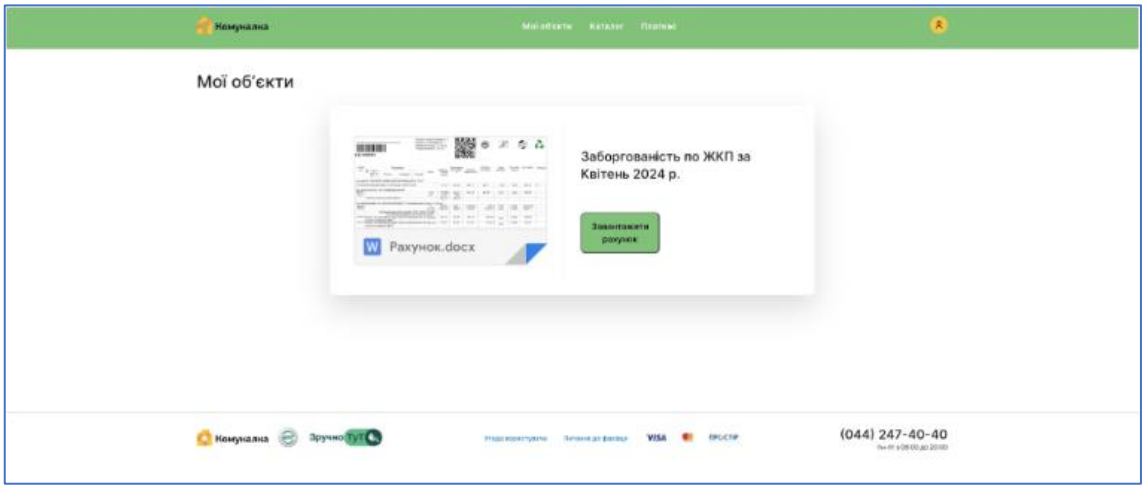


Figura 1 – Solicitação de download do arquivo malicioso “Заборгованість по ЖКП.rar”.

No processo de correção, foi possível recuperar e analisar a carga maliciosa contida no arquivo RAR “Заборгованість по ЖКП.rar”. Este arquivo RAR, quando baixado, revelou uma série de arquivos, um dos quais tinha um nome que incluía o caractere Unicode “U+201F”. Este caractere é exibido como um espaço em branco em dispositivos Windows e pode ser empregado para “esconder” extensões de arquivo, adicionando espaços em branco excessivos entre o nome do arquivo e sua extensão. Como ilustrado na Figura 2 (destacado em azul), este arquivo de nome enganoso dentro do arquivo RAR aparenta ser um documento PDF, mas na realidade é um arquivo CMD malicioso (“Рахунок на оплату.pdf[caractere unicode U+201F].cmd”).

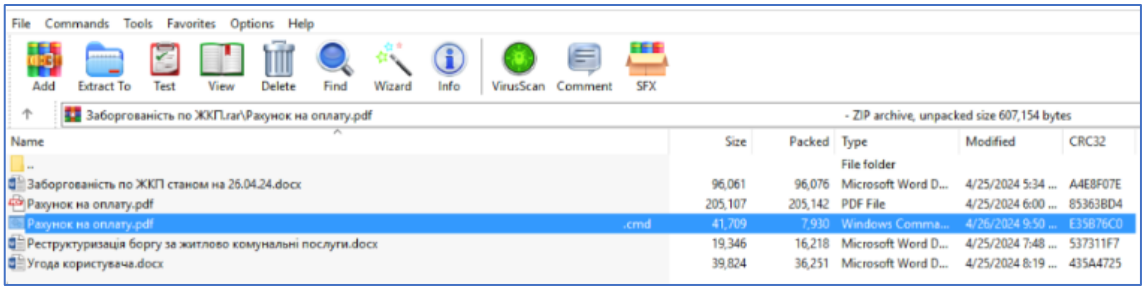
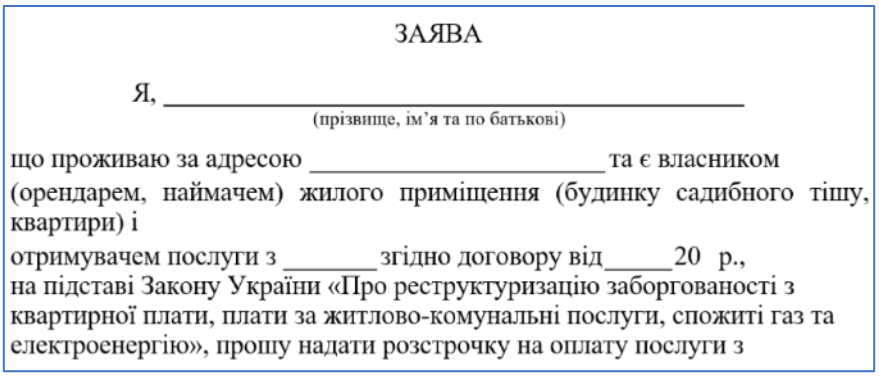


Figura 2 – Arquivos contidos no arquivo RAR malicioso “Заборгованість по ЖКП.rar”.

Foi adicionado um PDF inofensivo ao arquivo, que tem o mesmo nome do arquivo CMD, mas sem o caractere unicode, “Рахунок на оплату.pdf” (“Fatura para pagamento.pdf”). O nome do diretório do arquivo, após descompactado, também é “Рахунок на оплату.pdf”. Essa coincidência de nomes entre o PDF inofensivo e o diretório permite ao ator explorar a vulnerabilidade WinRAR CVE-2023-38831. Quando um arquivo contém um arquivo inofensivo com o mesmo nome do diretório, o WinRAR abre todo o conteúdo do diretório, resultando na execução do CMD malicioso. Ou seja, quando o alvo pensa que está abrindo o PDF inofensivo “Рахунок на оплату.pdf”, o arquivo CMD malicioso é ativado.

O arquivo CMD contém o malware COOKBOX do FlyingYeti PowerShell. Este malware foi criado para persistir em um host, atuando como um ponto de apoio no dispositivo infectado. Uma vez instalado, essa variante do COOKBOX fará solicitações ao domínio DDNS postdock[.]serveftp[.]com para C2, aguardando cmdlets do PowerShell que serão executados pelo malware. Junto com o COOKBOX, vários documentos falsos são abertos, contendo links de rastreamento ocultos usando o serviço Canary Tokens. O primeiro documento, mostrado na Figura 3 abaixo, se apresenta como um acordo sob o qual a dívida de habitação e serviços públicos será reestruturada.



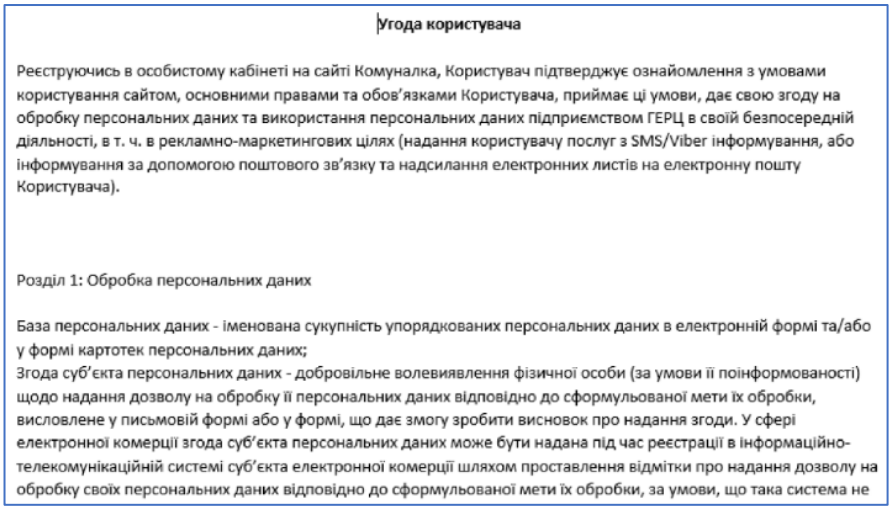
ЗАЯВА

Я, _____
(прізвище, ім'я та по батькові)

що проживаю за адресою _____ та є власником (орендарем, наймачем) жилого приміщення (будинку садибного тіпу, квартири) і
отримувачем послуги з _____ згідно договору від_____20 р.,
на підставі Закону України «Про реструктуризацію заборгованості з квартирної плати, плати за житлово-комунальні послуги, спожиті газ та електроенергію», прошу надати розстрочку на оплату послуги з

Figura 3 – Documento de restruturação de dívida.

O documento seguinte, é um acordo de usuário que detalha as regras e diretrizes para a utilização da plataforma de pagamento komunalka[.]ua.



Угода користувача

Реєструючись в особистому кабінеті на сайті Комуналка, Користувач підтверджує ознайомлення з умовами користування сайтом, основними правами та обов'язками Користувача, приймає ці умови, дає свою згоду на обробку персональних даних та використання персональних даних підприємством ГЕРЦ в своїй безпосередній діяльності, в т. ч. в рекламно-маркетингових цілях (надання користувачу послуг з SMS/Viber інформування, або інформування за допомогою поштового зв'язку та надсилання електронних листів на електронну пошту Користувача).

Розділ 1: Обробка персональних даних

База персональних даних - іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних;
Згода суб'єкта персональних даних - добровільне волевиявлення фізичної особи (за умови її поінформованості) щодо надання дозволу на обробку її персональних даних відповідно до сформульованої мети їх обробки, висловлене у письмовій формі або у формі, що дає змогу зробити висновок про надання згоди. У сфері електронної комерції згода суб'єкта персональних даних може бути надана під час реєстрації в інформаційно-телекомунікаційній системі суб'єкта електронної комерції шляхом проставлення відмітки про надання дозволу на обробку своїх персональних даних відповідно до сформульованої мети їх обробки, за умови, що така система не

Figura 4 – Documento de contrato do usuário.

A utilização de documentos forjados significativos, como parte das ações de phishing e entrega, é possivelmente uma tentativa dos operadores do FlyingYeti de melhorar a percepção de legitimidade de suas operações.

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 uma proteção antivírus

- Um pacote de software antivírus eficiente é o principal componente das defesas tecnológicas que todos os sistemas de computadores pessoais e comerciais devem ter.

Mantenha o sistema operacional e os aplicativos atualizados

- As atualizações frequentemente incluem patches de segurança que fecham as vulnerabilidades que os malwares podem explorar.

Evite clicar em links ou anúncios suspeitos

- Os malwares podem entrar em seu dispositivo quando você clica em um link ou anúncio infectado.

Não abra anexos de e-mail desconhecidos

- Muitos malwares se espalham através de anexos de e-mail. Se você não reconhece o remetente, é melhor não abrir o anexo.

Promova treinamentos e capacitações técnicas

- É importante treinar todos os funcionários sobre as melhores práticas de segurança cibernética. Isso pode incluir como identificar e evitar possíveis ameaças.

Adote estratégias de vigilância

- Qualquer processo diário ou solução utilizada pelo colaborador pode servir de porta de entrada para o malware, portanto o setor de tecnologia deve ter estratégias e protocolos para detecção de vulnerabilidades.

Crie uma cultura de responsabilidade

- É essencial que os colaboradores entendam os perigos do ataque de um malware e se preocupem legitimamente com isso. Portanto, é papel da organização estimular o senso de responsabilidade em funcionários de todos os setores.

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	
URL	hxxps[:]//github[.]com/komunalka/komunalka[.]github[.]io hxxps[:]//trabalhador-polido-union-f396[.]vqu89698[.]trabalhadores[.]dev hxxps[:]//raw[.]githubusercontent[.]com/kudoc8989/project/main/Заборгованість по ЖКП.rar hxxps[:]//1014[.]filemail[.]com/api/file/get?filekey=e_8S1HEnM5Rzhy_jpN6nL-GF4UAP533VrXzgXjxH1GzbVQZvmpFzrFA&pk_vid=a3d82455433c8ad11715865826cf18f6 hxxps[:]//pixeldrain[.]com/api/file/ZAJxwFFX?download= hxxp[:]//canarytokens[.]com/stuff/tags/ni1cknk2yq3xfcw2al3efs37m/payments.js hxxp[:]//canarytokens[.]com/stuff/terms/images/k22r2dnjrvjsme8680ojf5ccs/index.html
Domínio	postdock[.]serveftp[.]com comunidade[.]github[.]io

Tabela 1 – 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**
- **Cloudflare**
- **Thehackernews**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH