Brasília, 20 de abril de 2023

Nota à imprensa

Em relação à matéria “Hacking de Governo”, publicada pelo The Intercept Brasil no dia 19 de abril de 2023, a Apura Cyber Intelligence S/A se posiciona, em nota oficial à imprensa, diante dos erros e falta de conhecimento do repórter Paulo Motoryn sobre o tema e solicita aos demais veículos o cuidado de verificar sempre a autenticidade das informações para não republicar matérias contendo erros tão relevantes.

Faremos isso passo-a-passo para um melhor entendimento:

1. A matéria afirma **“Segundo o estudo “Mercadores da Insegurança”, do Instituto de Pesquisa em Direito e Tecnologia do Recife, a empresa está entre os três maiores players nacionais na intermediação da venda de ferramentas de hacking governamental.”**

Vale esclarecer alguns conceitos. Uma ferramenta de hacking é uma solução intrusiva de invasão. Já uma solução de segurança, como a ferramenta vendida para a Abin, é uma ferramenta de monitoração para acompanhar se a organização está sendo vítima de ameaças ou ataques cibernéticos.

Todas as organizações devem se prevenir de ataques e ameaças cibernéticas, dentro da lei. É fundamental para que elas evitem prejuízos inestimáveis e protejam a segurança de seus clientes e usuários. Essas ferramentas de segurança cibernética não têm nenhuma relação com ferramenta de hacking e a Apura Cyber Intelligence S/A jamais comercializou uma ferramenta como essa.

2. **“Pela descrição do serviço do Augury, a TeamCymru desenvolve sua tecnologia com base em um mecanismo de acesso ilegal e malicioso a dados de navegação e comunicações privadas, bem como dados referentes ao tráfego de internet. É muito claro concluir que a Abin está contratando uma organização criminosa. Essa conclusão é possível e logicamente comprovada pelo fato de o modelo de negócios da empresa ser baseado em coleta ilegal de dados”, afirmou o pesquisador André Ramiro.**

O produto da TeamCymru possui certificação ISO 27001 e está de acordo com a GDPR (General Data Protection Regulation ou Regulamento Geral de Proteção de Dados) e demais leis de privacidade.

A certificação ISO 27001 é uma das mais rigorosas de segurança da informação e atesta que a ferramenta preenche todos os requisitos para a proteção da informação, justamente o contrário do alegado pelo The Intercept.

Temos compromisso técnico com o aumento da segurança das empresas e do nosso país.

A revenda de produto para a Abin trata de ferramenta para segurança da informação. Ao contrário do publicado na matéria, a ferramenta auxilia no aumento de segurança cibernética e na proteção de ataques cibernéticos realizados e, de forma alguma, aborda monitoramento de redes sociais ou informações pessoais de cidadãos, além de não abrir informações criptografadas e não disponibilizar conteúdo de comunicações. O link do próprio fabricante aponta para isso - https://www.team-cymru.com/post/team-cymru-myth-vs-fact ou https://www.team-cymru.com/post/team-cymru-fatos-vs-mitos (versão em português).

3. "Nem isso fez a revendedora brasileira Apura deixar de exibir, em seu site oficial, o Team Cymru como "principal parceiro tecnológico". Até março, a página também exibia a Abin como "cliente", apesar da confidencialidade do contrato. O Intercept detectou, por meio da ferramenta WebArchive, que a menção à agência de inteligência estatal brasileira foi deletada em março – depois do início da apuração para esta reportagem."

Atualmente, 95% dos contratos são com empresas privadas. Nosso principal produto é o BTTng, plataforma de threat intelligence e antifraude, desenvolvida pela Apura, que é responsável por praticamente todos os nossos contratos hoje. Porém, a parceria com o Team Cymru continua existindo e os produtos deles serão comercializados quando for de entendimento do cliente que esta é a solução ideal.

Quanto à Abin, esse não foi o primeiro contrato firmado com a organização. Já tivemos outros contratos com a Abin e nem todos eram sigilosos. Por isso, a Abin figurava em nosso site.

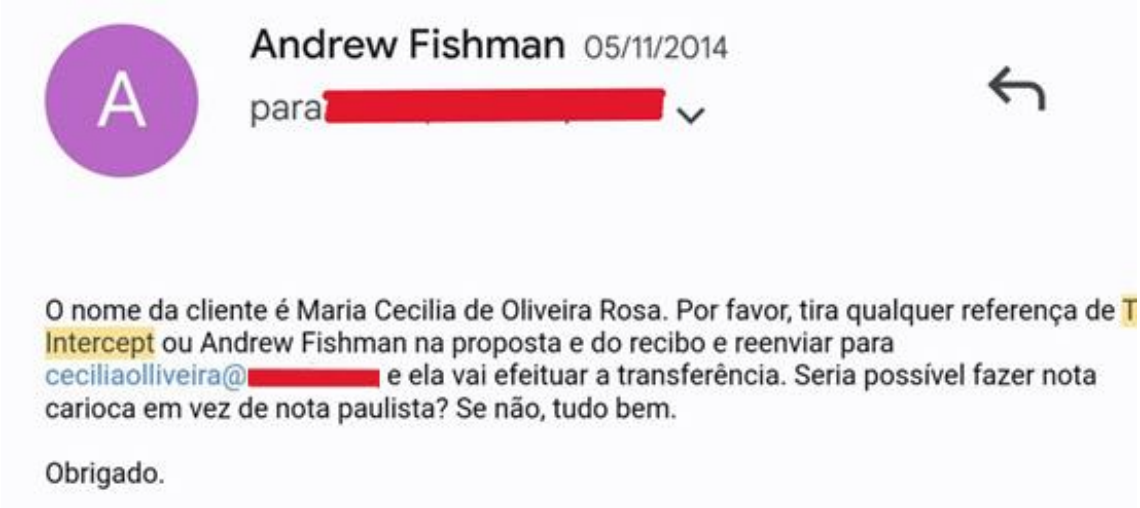
Ressaltamos também que o repórter Paulo Motoryn fez o primeiro contato com a Apura no dia 17 de abril de 2023. Apenas nessa ocasião ficamos sabendo desta matéria e nenhuma alteração no nosso site foi feita decorrente disso.

4. "Ao Intercept, a Apura afirmou que revendeu produtos para a Abin em 2015 e em 2020. "Todas as ferramentas ofertadas nesses contratos são de segurança da informação e seguem estritamente este escopo", disse a empresa. A Apura garante que "nenhuma das ferramentas ofertadas para a Abin possibilitam acessar o conteúdo de e-mails e redes sociais de cidadãos", como diz o fabricante."

É fundamental para o Brasil ser capaz de monitorar ameaças e ataques a infraestruturas críticas e a Apura Cyber Intelligence S/A tem compromisso técnico com o aumento da segurança das empresas e do nosso país, independente do momento político que o país está.

Uma ferramenta de segurança cibernética, como explicado no início do documento, é uma ferramenta de monitoração para acompanhar se a organização está sendo vítima de ameaças ou ataques cibernéticos.

O próprio The Intercept Brasil já contratou produto de forense computacional com a Apura Cyber Intelligence S/A, em 2014, sabendo da importância de uma segurança cibernética para a empresa. Na época, o contato foi feito com o Sr. Andrew Fischmen, que nos solicitou que a nota fiscal fosse emitida em nome da jornalista Maria Cecilia de Olliveira Rosa, conforme mostram as imagens abaixo.



Andrew Fishman 05/11/2014

para [redacted]

O nome da cliente é Maria Cecilia de Oliveira Rosa. Por favor, tira qualquer referença de T Intercept ou Andrew Fishman na proposta e do recibo e reenviar para ceciliaolliveira@[redacted] e ela vai efeituar a transferência. Seria possível fazer nota carioca em vez de nota paulista? Se não, tudo bem.

Obrigado.

---------- Forwarded message ---------

De: [redacted]

Date: qua., 5 de nov. de 2014 18:31

Subject: Fwd: Fwd: Procura: Intella Pro Dongle

To: Andrew Fishman <andrewdfishman@[redacted] ceciliaolliveira@[redacted]

Cc: [redacted]

Andrew, Boa Tarde !

Segue nova proposta e nova Nota Fiscal.

Com esses esclarecimentos, a Apura Cyber Intelligence S/A lamenta a divulgação à imprensa que foi sensacionalista e que não condiz com a verdade dos fatos.

A Apura está sempre disposta a colaborar com informações para um jornalismo responsável e consciente. Estamos à disposição para dúvidas ou esclarecimentos, mas prezamos pela veracidade dos fatos.

ANEXO 1 – Material publicado pelo Team Cymru em https://www.team-cymru.com/post/team-cymru-fatos-vs-mitos

Team Cymru Fatos vs Mitos

O Team Cymru tem uma missão clara: *Salvar e Melhorar Vidas Humanas.* Nós nos esforçamos para cumprir essa missão, equipando os defensores de rede com insights provenientes de métricas de Internet, que processamos e refinamos esses dados em uma forma útil de inteligência de ameaças.

Ocorrem mal-entendidos sobre o uso de métricas de tráfego de Internet para proteger as redes de ataques e abusos. Este post procura esclarece como coletamos, refinamos e distribuímos inteligência de ameaças derivadas de dados provenientes da Internet.

Fazemos isso para nossos clientes e para a comunidade de defensores da segurança na Internet, que acreditam em tornar a Internet mais segura para todos. Esperamos que este post ajude a explicar a missão que temos perseguido apaixonadamente por mais de 20 anos.

MYTHS *A Team Cymru é um 'corretor de dados[1]'*

FACTS ***Fato: Nós não somos um corretor de dados.***

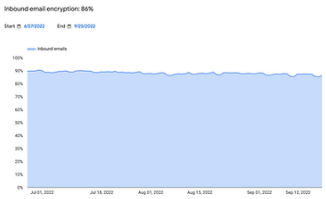
Nosso foco está em dispositivos de Internet comprometidos e malévolos, não em pessoas. Não mantemos dados de assinantes que permitam que qualquer usuário de nosso produto conecte uma pessoa a uma parte da infraestrutura da Internet. Os dados que sustentam o nosso produto são legalmente tratados e estão em conformidade com todos os regulamentos de privacidade de dados aplicáveis, incluindo GDPR, CCPA e outras legislações de privacidade estaduais e nacionais relevantes. Nossa plataforma não mostra o tipo, o uso ou os usuários dos serviços de Internet.

MYTHS *Mito: A plataforma Augury disponibiliza uma ampla gama de diferentes tipos de dados da Internet para seus usuários, incluindo dados de captura de pacotes (PCAP) relacionados a e-mail, área de trabalho remota e protocolos de compartilhamento de arquivos.*

FACTS ***Fato: Nossa plataforma não coleta e-mail, área de trabalho remota ou compartilhamento de arquivos (FTP, torrents, et al.) na Internet.***

Numerosos estudos mostraram que a coleta de e-mails não é possível porque a grande maioria dos e-mails é criptografada de ponta a ponta. Em um relatório do Google de setembro de 2022 [2], foi mostrado que 75% dos e-mails de saída e 86% dos e-mails de entrada são

Numerosos estudos mostraram que a coleta de e-mails não é possível porque a grande maioria dos e-mails é criptografada de ponta a ponta. Em um relatório do Google de setembro de 2022 [2], foi mostrado que 75% dos e-mails de saída e 86% dos e-mails de entrada são



criptografado em trânsito. O e-mail enviado e recebido para muitos provedores, como Google, Microsoft, Cloudflare, Amazon, Comcast, Apple iCloud, Facebook, LinkedIn, Twitter, Instagram e Protonmail, é criptografado em trânsito por padrão via TLS, sem qualquer configuração de usuário necessária. De acordo com a Microsoft [3], o Protocolo de Ambiente de Trabalho Remoto (RDP) tem sido encriptado por predefinição desde 2009.

Extraímos endereços de e-mail maliciosos (não o conteúdo), tentativas de acesso à área de trabalho remota e tentativas de acesso à FTP por meio de nossas sandbox de malware, e relatamos spam e phishing de nossas armadilhas de spam e honeypots. Todos os nossos PCAPs são gerados em nossa própria infraestrutura interna.

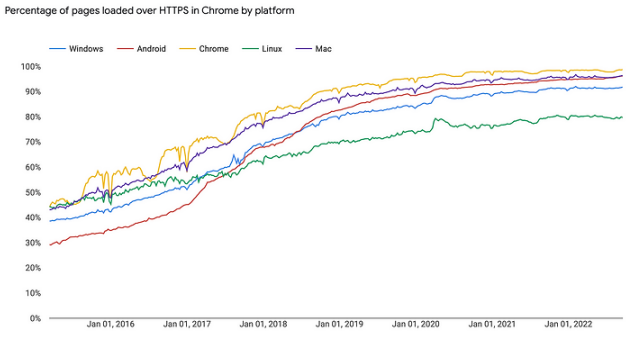
MYTHS

Mito: "Os dados da Augury também podem incluir atividades do navegador da Web, como URLs visitadas e uso de cookies".

FACTS

Fato: Nossa plataforma não é capaz de coleta e apresentação de tráfego da Web global. Nossa plataforma fornece apenas URLs e cookies mapeados para servidores maliciosos.

Estudos provaram que essa atividade de coleta simplesmente não é possível. A web é uma esfera criptografada, mantendo o tráfego da web a salvo de olhares indiscretos. O estudo de transparência do Google [4] mostra que mais de 90% dos carregamentos de páginas através do navegador Chrome são criptografados por HTTPS. Na revisão do Google dos 100 principais sites, que respondem por 25% de todo o tráfego global da web, 100 em cada 100 desses sites fornecem criptografia e 97 deles têm como padrão a criptografia. Scott Helme [5] realizou verificações do Alexa top um milhão de sites, e mostrou que 72% dos principais um milhão de sites padrão para criptografia. O Conselho de Segurança da CA [6] previu que mais de 90% do tráfego da web seria criptografado até maio de 2019, combinando previsivelmente as descobertas atuais do Google. O projeto de Telemetria do Firefox *[7] concluiu que 87% de todos os carregamentos de páginas pelos navegadores Firefox foram criptografados.*



SÃO PAULO
Av Paulista, 2.421,
1º andar, Jardins
CEP: 01310-300
11 5504-1966

BRASÍLIA
SHN Quadra 1 Lote A Bloco A
Edifício Le Quartier, 14º andar
CEP: 70077-000
61 3255-1245

0800 719 1902
apura.com.br
linkedin.com/company/apura

No entanto, existem sites comprometidos, com o estudo Webtribunal [8] de abril de 2022 observando que 1 em cada 10 URLs são maliciosas. A IBM observou [9] em 2020 que 30.000 sites são hackeados todos os dias. Por meio de nossos mecanismos de análise de malware, scanners, honeypots, armadilhas de spam, detecção de phishing, plataforma IDS e feeds de IOCs (indicadores de comprometimento), identificamos sites comprometidos. Esses sites espalham malware, comandam exércitos de bots e lançam ataques, além de roubar credenciais. Os defensores de rede querem detectar, bloquear ou limpar esses dispositivos e dispositivos infectados relacionados o mais rápido possível. Nossa plataforma torna possível ver esses sites que foram hackeados. Esses dados estão vinculados exclusivamente a atividades maliciosas e infraestrutura maliciosa, e os defensores da rede que usam nossas ferramentas dependem deles para defender melhor sua própria infraestrutura.

MYTHS

Mito: A equipe Cymru obtém dados PCAP dos ISPs com os quais tem relacionamentos.

FACTS

Fato: Nós não obtemos dados PCAP de qualquer 3ª parte.

Investimos recursos significativos para executar nossa própria plataforma global de honeypots, sensores IDS, scanners e vários mecanismos de processamento de malware. Nossa infraestrutura é a fonte de nossos dados. Esses dados formam a base de nossos produtos e serviços, incluindo serviços gratuitos como nosso Programa de Assistência à CSIRTs (Computer Security Incident Response Team) e o Registro de Hash de Malware (MHR). As equipes da CSIRT em mais de 154 países baixam nossa inteligência de ameaças diariamente sem custo. Milhões de consultas chegam aos nossos portais de insights disponíveis publicamente e nossos clientes usam nossos feeds e plataformas para defender suas redes. Nossa reputação estelar resulta de duas décadas de parceria com as comunidades e defensores da rede.

MYTHS

Mito: "Augury também contém os chamados dados netflow ... Os registros Netflow podem revelar a quais servidores os usuários se conectam, muitas vezes revelando sites específicos que visitam. Os registros também podem revelar o volume de dados enviados ou recebidos e por quanto tempo um usuário acessou um site.

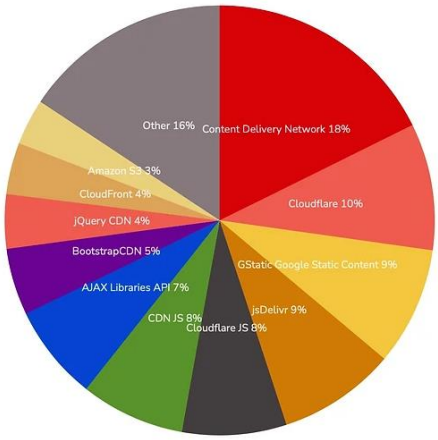
FACTS

Fato: Augury não fornece a ninguém acesso a dados brutos ou de fluxo de rede em massa. Os registros Netflow não contêm conteúdo ou informações do usuário. É estatisticamente impreciso afirmar que o netflow pode ser usado para identificar um indivíduo ou fornecer um padrão de vida que pode ser mapeado para uma pessoa e preferências.

Consultas limitadas e específicas que produzem resultados anônimos e agregados podem ser derivadas do netflow amostrado. O Netflow não identifica usuários. Os dados do Netflow incluem apenas cabeçalhos, como endereços IP de protocolo e dispositivo. É amostrado e, portanto, vê apenas aproximadamente 1 em cada 10.000 fluxo. Essas sessões incluem varredura, hacking, DDoS e outras formas de atividade maliciosa. Além disso, as sessões legítimas são conduzidas através de redes de entrega de conteúdo (CDN) atrás das quais estão milhões de sites. Dos 1 milhões de principais sites [10 *], 43,96% ficam atrás de CDNs, 59,04% dos 100 principais sites e 61,95% dos 10 principais sites. É impossível usar o netflow para diferenciar entre esses sites. Além disso, a infraestrutura compartilhada entre provedores de nuvem impede ainda mais a identificação de infraestruturas hospedadas em nuvem específicas. Portanto, é estatisticamente impreciso afirmar que o netflow pode ser usado para identificar um indivíduo ou fornecer um padrão de vida que possa ser mapeado para uma pessoa e preferências. Não há logs ou qualquer conteúdo incluído no netflow.*

CDN Usage Distribution in the Top 1 Million Sites

Distribution for websites using CDN technologies



Controladores maliciosos, varreduras em larga escala e DDoS têm uma persistência e periodicidade que revela um padrão estatístico, permitindo o mapeamento de infraestruturas maliciosas e identificando dispositivos hackeados de importância para os defensores da rede. Augury permite o mapeamento de dispositivos maliciosos, não de pessoas. Consulte nosso Monitor de Ameaças Nimbus e outros Serviços Comunitários *para obter detalhes adicionais. https://www.team-cymru.com/community-services [11]*

MYTHS

Mito: "Augury fornece diferentes níveis de acesso para clientes privados (comerciais) e governamentais.

FACTS

Fato: Falso. Há uma plataforma idêntica com camadas baseadas em uso.