NOZOMI NETWORKS LABS

Sumário Executivo

Relatório de segurança OT/IoT

Percepções sobre guerra cibernética, ameaças e tendências, recomendações

Revisão do primeiro semestre de 2022 | Publicação de Agosto

Sumário Executivo

Com o cenário de ameaças cibernéticas em constante mudança, é mais importante do que nunca entender como isso está impactando sua organização. Nos últimos seis meses, presenciamos um crescimento repentino na frequência e na complexidade de ataques, bem como o uso de novas táticas por parte dos agentes de ameaças. Ameaças que uma vez eram consideradas improváveis repentinamente se tornaram lugar comum.

Por exemplo, as empresas que anteriormente não eram alvos de ransomware estão agora recebendo esses ataques. Além dessa mudança, os agentes de ameaças continuam a dissimular suas atividades ilícitas para dificultar sua detecção pelas soluções de segurança.

Para reforçar a segurança e minimizar as ameaças futuras, as empresas precisam de percepções em tempo real sobre sua exposição de risco cibernético para que possam tomar decisões bem fundamentadas sobre a melhor maneira de se protegerem.

Neste relatório nós:

- **Analisamos** o estado atual da cibersegurança.
- **Identificamos** as principais tendências no cenário de ameaças e oferecemos soluções para enfrentá-las.
- **Recapitulamos** a guerra entre a Rússia e a Ucrânia, destacando as novas ferramentas mal-intencionadas e malware introduzidos, bem como de que forma esse conflito pode nos dar informações sobre as capacidades dos atacantes.
- **Fornecemos** informações sobre botnets da Internet das Coisas (IoT), indicadores de comprometimento (IoCs) correspondentes e Técnicas e Procedimentos Táticos (TTPs) dos agentes de ameaças.
- **Compartilhamos** recomendações e análise de previsões.

CENÁRIO DE AMEÇAS DO PRIMEIRO SEMESTRE DE 2022

Desde o início da invasão da Ucrânia pela Rússia em fevereiro, nós testemunhamos:

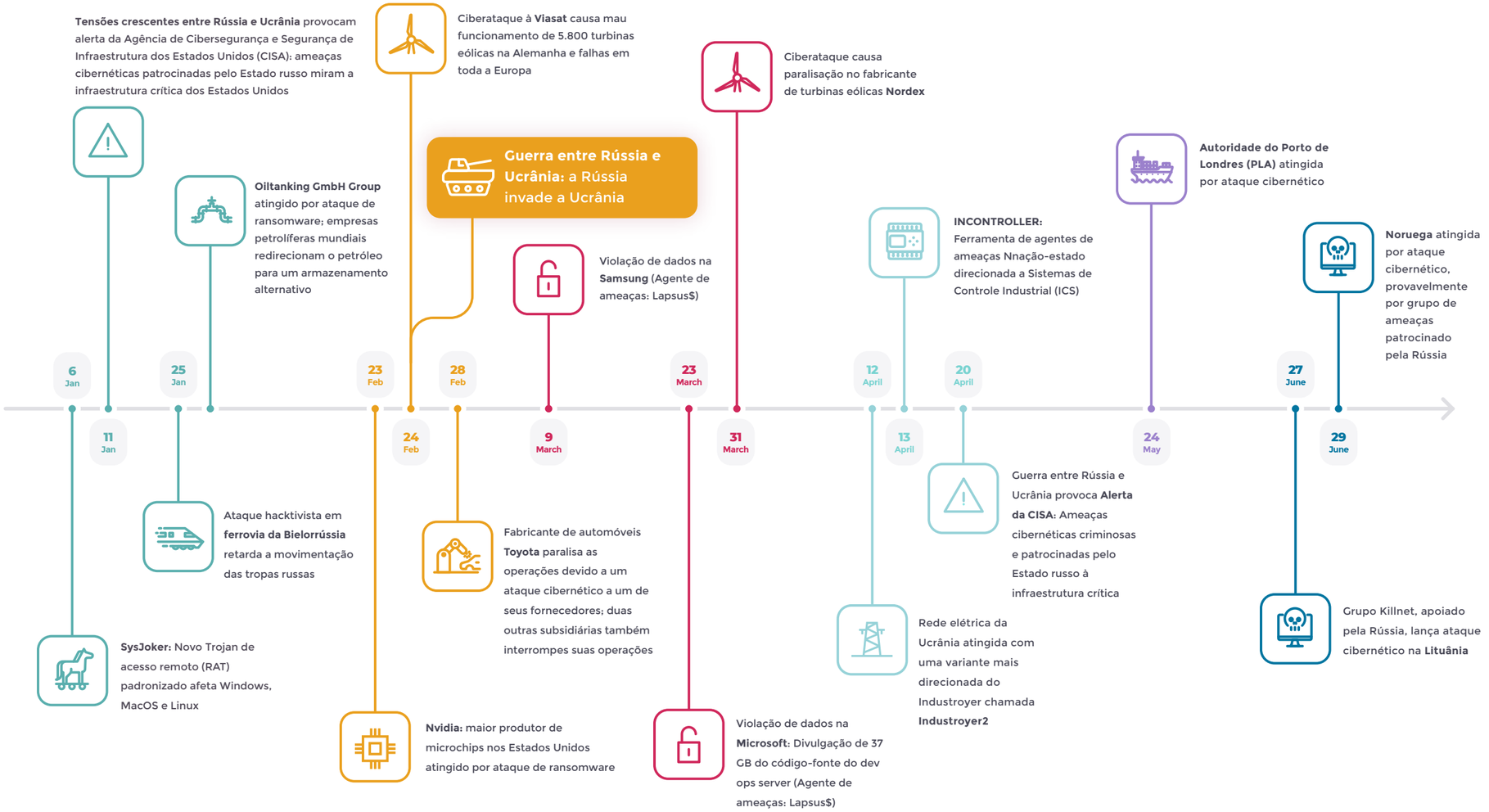
- **Atividade hacktivista**
- **APTs patrocinados pelo Estado e cibercriminosos**
- **Malware wiper**
- **Industroyer2**

Cronograma dos eventos cibernéticos de destaque no primeiro semestre de 2022

O cronograma desta página destaca vários eventos cibernéticos significativos ocorridos entre janeiro e junho de 2022 e que definiram o atual cenário de ameaças.

Desde o início da invasão da Ucrânia pela Rússia, em fevereiro de 2022, testemunhamos atividades de vários tipos de agentes de ameaças, inclusive hacktivistas, APTs patrocinadas pelo Estado e cibercriminosos.

Também vimos o uso robusto de malware wiper, além do desenvolvimento de uma variante do Industroyer, batizada de Industroyer2 destinada a para o uso impróprio do protocolo IEC-104, comumente utilizado em ambientes industriais.



Cenário da Botnet IoT

Os honeypots da Nozomi Networks Labs coletam dados que, ao serem analisados, fornecem algumas percepções interessantes sore a atividade de um agente de ameaças. Na primeira metade de 2022, observamos as seguintes tendências:

- **Principais países de origem de ataques:** As principais atividades cibernéticas vêm de endereços de IP associados à China e aos Estados Unidos. Suas superfícies de invasão são provavelmente devidas a sua tecnologia sofisticada e suas indústrias manufatureiras.
- **Protocolos envolvendo credenciais embutidas em códigos:** Mirai é uma botnet popular que, originalmente, fazia uso impróprio do Telnet, mas que após os agentes de ameaças liberarem o código-fonte ao público foi modificada para mirar SSH e outros protocolos.
- **Principais credenciais usadas:** as credenciais "root" e "admin" são alvos atraentes óbvios usados em diversas variações, pois podem permitir que agentes de ameaças acessem todos os comandos do sistema e contas de usuários.
- **Maior quantidade de endereços de IP de invasor único:** Segundo os endereços de IP associados a atividade mal-intencionada coletados por nossos honeypots, abril foi o mês mais ativo, com a coleta de quase 5.000 endereços de IP de invasor único.
- **Principais comandos executados:** Identificamos os 10 comandos mais executados com `habilitar`, `shell`, `sistema` `eque` é formando a lista. Aproximadamente 12.500 botnets executaram cada um desses comandos.

Abril
foi o mês mais ativo para botnets com quase

5.000
endereços de IP de invasor único coletados.

Leia o **Relatório completo** para ver mais sobre a atividade de botnet de IoT no primeiro semestre de 2022.

O cenário de vulnerabilidades

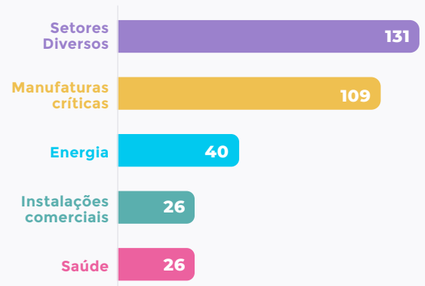
A postura de segurança de muitos produtos de software e hardware para ICS é exposta por meio das vulnerabilidades descobertas principalmente por pesquisadores de segurança. No primeiro semestre de 2022, ocorreram 560 vulnerabilidades e exposições comuns (CVEs) emitidas por ICS-CERT, das quais 303 foram divulgadas recentemente. Houve 14% menos CVEs reportadas em comparação com o segundo semestre de 2021.

131 das CVEs reportadas afetaram vários setores. A manufatura crítica foi o setor mais diretamente afetado, com 109 CVEs reportadas. Energia foi o segundo, com 40, e as instalações comerciais e de saúde e vieram em terceiro lugar, com 26. Além disso, 60 fornecedores diferentes foram mencionados em consultorias de CVE, com 172 produtos associados. Desde o segundo semestre de 2021, houve um aumento de 27% nos fornecedores afetados e de 19% nos produtos afetados.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

560
CVEs emitidas

SETORES MAIS IMPACTADOS



Recomendações

Existe uma necessidade crescente de tomar medidas de segurança proativas que possam ser implementadas pelas diferentes partes envolvidas dentro de uma organização. Isso inclui equipes de TI, executivos de compliance e gerentes de riscos, que podem ter perspectivas diferentes sobre questões de segurança. As práticas prioritárias de segurança devem incluir:

- Manutenção de um inventário preciso dos ativos
- Implementação dos patches mais recentes em tecnologia VPN
- Gestão dos acessos privilegiados
- O uso de Autenticação Multifator (MFA) que não seja suscetível a vishing ou SIM swapping
- Troca frequente de senhas, e
- Maior treinamento dos funcionários sobre vishing e engenharia social como um todo

Mitigações adicionais:

- **Backups:** Para evitar que um ransomware ou um ataque de malware wiper resulte em perda completa de dados, faça backup de seus dados regularmente, teste seu sistema de backup e assegure-se que seu backup seja armazenado em um local externo e não na mesma rede dos servidores operacionais.
- **Inteligência de ameaças:** Inteligência de ameaças cibernéticas é a prática de coletar, analisar e disseminar informações sobre as ciberameaças para ajudar as organizações a proteger seus sistemas e dados. Essas informações podem incluir assinaturas de malware, vetores de ataque e indicadores de comprometimento (IoCs).
- **Segurança em nuvem:** Verifique se seu provedor de nuvem tem uma reputação sólida e esteja em conformidade com os padrões do setor, como a ISO 27001 ou as certificações SOC 1/2/3, que criptografe os dados que estiverem sendo armazenados ou transferidos e que use o 2FA e ferramentas de gestão de identidade.
- **Detecção de ameaças:** A detecção de ameaças é usada para detectar e responder a ameaças potenciais em tempo real, bem como para fornecer alertas sobre eventos futuros. Na detecção de ameaças, os sistemas monitoram a rede em busca de atividades suspeitas, como um volume incomum de tráfego vindo de um endereço IP ou um grande número de conexões a um determinado serviço. Isso pode ser feito observando-se atividade anormal ao longo do tempo ou escaneando a rede para verificar vulnerabilidades conhecidas.
- **Software Bill of Materials (SBOM):** O SBOM proporciona uma ideia de quantas versões diferentes existem de cada componente e de onde elas são usadas, permitindo assim rastrear as mudanças ao longo do tempo e assegurar que elas não causem problemas com outros componentes. Ele também pode ajudar a entender quais componentes estão mais expostos ou mais vulneráveis do que outros, e como mitigar tais vulnerabilidades. Apesar de os SBOMs ainda não serem amplamente utilizados, vale a pena acompanhar o desenvolvimento dessa tecnologia.

PRINCIPAIS MITIGAÇÕES DE AMEAÇAS PARA MAIOR SEGURANÇA

- Backups
- Inteligência de ameaças
- Segurança em nuvem
- Detecção de ameaças
- Software Bill of Materials

Previsão

Com base nesta última análise, apresentamos abaixo algumas das principais tendências em segurança cibernética que esperamos ver até o final de 2022:

- Mais ataques relacionados a ICS
- Agentes de ameaças de ransomware continuarão a visar empresas de infraestrutura crítica
- Mais ataques voltados a empresas maiores
- Roubo de código-fonte de tecnologia
- Um aumento nas políticas e governança cibernética, conforme as iniciativas privadas/governamentais estabelecidas mais no início deste ano tomarem forma

Baixe o Relatório de segurança OT/IoT

A Nozomi Networks Labs analisa o atual cenário de ameaças e compartilha:

- Ataques recentes de ransomware e botnet de IoT
- ICS, vulnerabilidade de dispositivos OT/IoT e tendências de exploração
- Etapas para melhorar suas estratégias de remediação de ciberameaças

Baixar

Nozomi Networks

A solução líder do setor para visibilidade e segurança de OT e IoT

A Nozomi Networks acelera a transformação digital protegendo a infraestrutura crítica mundial e as organizações industriais e governamentais contra ameaças cibernéticas. Nossa solução proporciona visibilidade excepcional da rede e dos ativos, detecção de ameaças e informações para ambientes de OT e IoT. Os clientes confiam em nós para minimizar o risco e a complexidade e, ao mesmo tempo, maximizar a resiliência operacional.

© 2022 Nozomi Networks, Inc.
Todos os direitos reservados.
NN-SEC-RP-ES-PT-2022-1H-001

nozominetworks.com