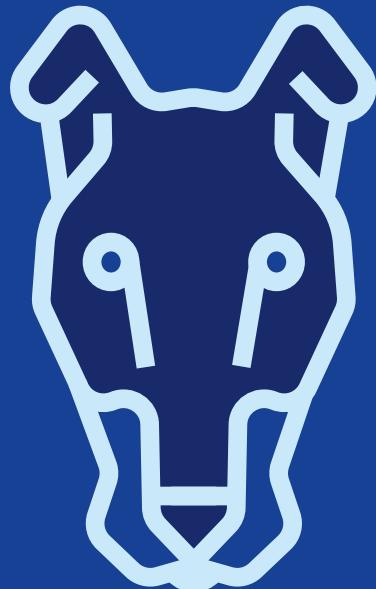


Cyber Bogies



nixu
cybersecurity.

Cyber Bogies are our gallery of “usual suspects” – malicious and otherwise troublesome people that may form a threat to IT systems or processes. The characters are based on stereotypes and caricatures, which make them memorable and easier to understand.

You can use Cyber Bogies as brainstorming help in threat workshops, backlog grooming, test planning, or design meetings.

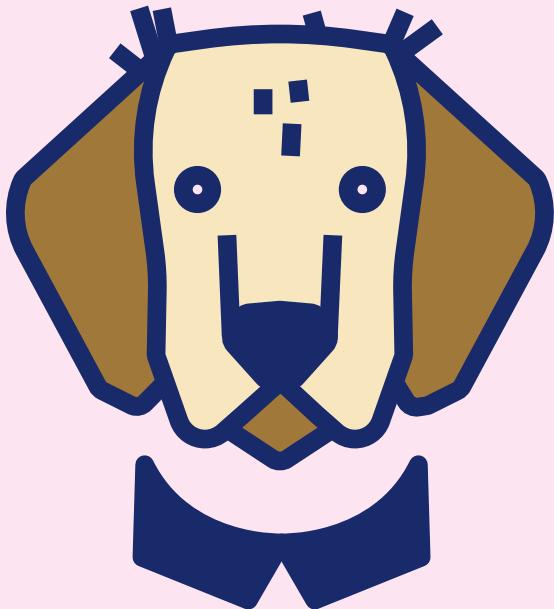
www.nixu.com



Nixu Cyber Bogies is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

OPPORTUNISTIC PASSER-BY “KEVIN” INTENTIONAL



01

nixu

OPPORTUNISTIC PASSER-BY “KEVIN”

Kevin is a man in his 20s interested in technology and likes to check out systems installed in public spaces or other accessible places. Kevin gets irritated when finding a bad or suspicious solution.

Motivation and goals

- Curiosity, learning, not necessarily malicious
- Might abuse a vulnerability accidentally or to “teach a lesson”

Targets

- Physical devices with user interfaces or connections
- Especially in public spaces

Skills and methods

- Some technical skills
- Push buttons and poke around in user interfaces
- Connect devices on USB, Ethernet, NFC or other standard connectors
- Remove cables

Resources and budget



Harm potential

- key Abuse of functionality
- cd Using ready-made tools

Attacks from

- locationNearby
- crossPhysical



Nixu Cyber Rogues is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

SCRIPT KIDDIE “JONNE” INTENTIONAL



02

nixu

SCRIPT KIDDIE “JONNE”

Jonne is a teenager who uses existing tools to exploit systems connected to the Internet. Jonne lives with his parents and spends his spare time online, hanging out in hacker forums.

Motivation and goals

- Curiosity, learning
- Bragging rights

Targets

- Any internet-facing system with known vulnerabilities

Skills and methods

- Find and install commonly used hacking tools
- No in-depth knowledge for developing own exploits or adapting existing ones

Resources and budget



\$\$\$\$\$

Harm potential



Abuse of functionality



Using ready-made tools

Attacks from



From internet



Nixu Cyber Bogies is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

SERVICE TECHNICIAN “ROHAN” INTENTIONAL



03

nixu

SERVICE TECHNICIAN “ROHAN”

Rohan works as a technician who installs and maintains systems on-site. Rohan is a subcontractor and works for multiple clients. He has access to the required tools and documentation.

Motivation and goals

- Cutting corners, **laziness**
- **Cover up mistakes** and negligence
- Snoop and sell information
- **Revenge** on the old employer

Targets

- Administrative interfaces in building infrastructure equipment (such as HVAC / fire alarm / building security systems / security cameras / industrial control systems / vehicles etc.)

Skills and methods

- Exploit loopholes and gaps in tools and processes with **insider knowledge**
- **Abuse account permissions**
- Abuse default or old active credentials
- Simple **web exploits**

Resources and budget



Harm potential

- Abuse of functionality
- Using ready-made tools

Attacks from

- Nearby
- Physical



Nixu Cyber Rogues is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

CLOUD ADMIN “CHARLOTTE” INTENTIONAL



04

nixu

CLOUD ADMIN “CHARLOTTE”

Charlotte is an administrator in a SaaS IT service company and has maintenance access to a multitude of customer systems with confidential data. To speed things up, Charlotte copies configuration between systems, takes test data from production, and makes direct changes to databases. To ensure sales case success, Charlotte might reveal details about existing customers.

Motivation and goals

- Maximize profit (optimize costs, maximize productivity)
- Competitive advantage
- Lock in current customers
- Poach good deals

Targets

- User interfaces
- Admin and maintenance functionality in cloud services
- Direct database and host access
- “Best test data is from production”

Skills and methods

- Abuse account permissions and application functionality
- Fail fast operations methodology
- Exploit process loopholes and logical flaws with **insider knowledge**
- Abuse lack of traceability

Resources and budget



\$\$\$\$\$

Harm potential



Abuse of functionality

Attacks from



From internet



Nixu Cyber Rogues is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

05

PETTY THIEF "KYLE" INTENTIONAL



nixu

PETTY THIEF "KYLE"

Kyle is a small-time criminal, financing his habits by stealing just about anything worth money that he can carry. Unsupervised laptop in the office? Was your phone left on the table? Kyle will see his opportunity and take it. You may find your belongings on sale on Facebook or eBay later.

Motivation and goals

- Money

Targets

- Any physical object of value
- Unsupervised tools: laptops, phones, instruments
- Parts and components: metals, electronic devices, spare parts, copper cables

Skills and methods

- May not understand what exactly he is stealing
- **Bolt cutters** and **hack saws**

Resources and budget



\$\$\$\$\$

Harm potential



Using ready-made tools

Attacks from



Physical



Nixu Cyber Rogues is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

MALWARE CAMPAIGN RUNNER “SERGEI” INTENTIONAL



06

nixu

MALWARE CAMPAIGN RUNNER “SERGEI”

Sergei is a cybercriminal working for an organized crime outfit somewhere in Eastern Europe. He scans the internet for potential targets for botnets, malware infection, and DDoS for ransom.

Motivation and goals

- Make as much **money** as possible with the smallest effort

Targets

- Any system connected to the internet: workstations, servers, IoT devices

Skills and methods

- Limited technical skills, typically using tools purchased from malware developers.
- **Ransomware**
- Extortion with **DDoS**
- Set up **botnets**
- Set up bitcoin mining **malware**

Resources and budget



Harm potential

Using ready-made tools

Attacks from

From internet



Nixu Cyber Rogues is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

PHISHING CAMPAIGN RUNNER "ANTONIA" INTENTIONAL



07

nixu

PHISHING CAMPAIGN RUNNER "ANTONIA"

Antonia is a cybercriminal working for an organized crime outfit somewhere in Latin America. She scans the internet for potential targets for phishing and information-stealing malware. Why have a day job if there are stupid users to fool?

Motivation and goals

- Make much **money** with little effort
- Gain material for future scams
- **Stealing identities**
- Stealing credentials

Targets

- Vulnerable internet-connected servers and websites, such as unpatched content management systems
- Users that can be fooled easily
- Any interesting credentials (online banking, credit cards, email accounts)

Skills and methods

- Limited technical skills, uses tools purchased from darknet
- Set up **phishing sites**
- Delivering **information-stealing malware**
- Search for unencrypted credentials or credit card numbers

Resources and budget



\$\$\$\$\$

Harm potential

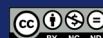


Using ready-made tools

Attacks from



From internet



Nixu Cyber Rogues is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

08

COMPETITOR R&D ENGINEER “JIN” INTENTIONAL



nixu

COMPETITOR R&D ENGINEER “JIN”

Jin works for a competitor company. Jin’s job is to reverse engineer products chosen by the supervisors for analysis. Jin enjoys the challenge of bypassing feeble firmware protections – the harder, the better.

Motivation and goals

- Works for salary
- Copy innovations
- Identify patent and license violations – **money**
- Likes the **challenge**

Targets

- Firmware and binaries for any physical device
- Protected applications for desktop or mobile
- Intellectual property of competitors
- Design documents

Skills and methods

- Advanced technical skills
- Able to extract local data from hardware
- **Reverse engineering** firmware and applications
- Can utilize debuggers and emulators

Resources and budget



\$\$\$\$\$

Harm potential



- Using ready-made tools
- Creates own exploits and tools

Attacks from



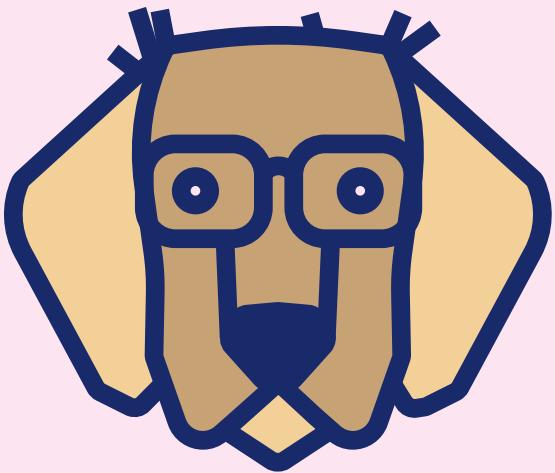
- From internet
- Physical



Nixu Cyber Rogues is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

STATE-SPONSORED AGENT “MAGIC HOUND” INTENTIONAL



09

nixu

STATE-SPONSORED AGENT “MAGIC HOUND”

A traditional state-sponsored operative aiming to acquire intelligence information or to get a foothold in critical infrastructure or computer systems of government agencies.

Motivation and goals

- **Cyberwarfare**, intelligence
- Harm critical infrastructure
- Spread **disinformation** and cause political disturbance
- Getting access to restricted environments or systems related to national security

Targets

- Critical infrastructure
- National security and government agencies
- Online voting systems
- Websites used by the target organization and subcontractors to create watering holes

Skills and methods

- Advanced technical skills, developing **complex exploits**
- **Supply chain attacks**, malware
- Wiretapping and **watering holes**
- Air gap jumping (malicious USB)
- Local presence and social engineering

Resources and budget



\$\$\$\$\$

Harm potential



Creates own exploits and tools

Attacks from



From internet



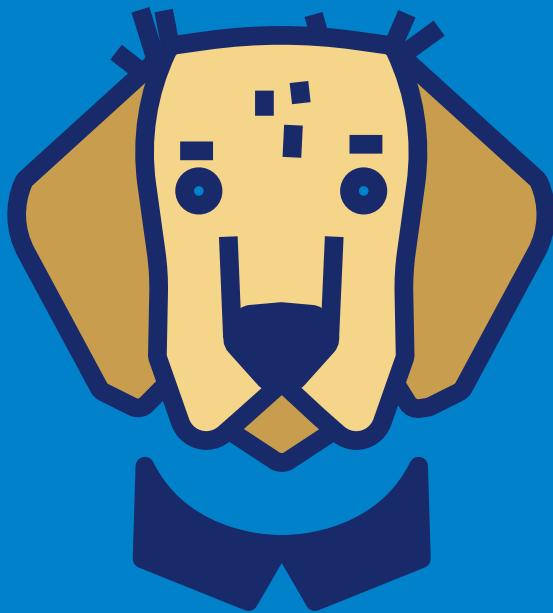
Physical



Nixu Cyber Bogies is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

CLUELESS EMPLOYEE “JOSH” UNINTENTIONAL



10

nixu

CLUELESS EMPLOYEE “JOSH”

Josh is a recent employee who has not been fully trained and does not always know what he is doing: if something can go wrong, it will. Josh will click without reading and ask questions later.

Motivation and goals

- Act first, think later or not at all
- Appear busy and clever
- Hide mistakes

Targets

- Misuse of permissions in all systems
- All systems that he interacts with

Skills and methods

- Human errors and mistakes
- Will misinterpret things and do things not supposed to do: delete data, overwrite critical things and so on

Resources and budget



Harm potential



Accidental

Attacks from



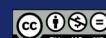
From internet



Nearby



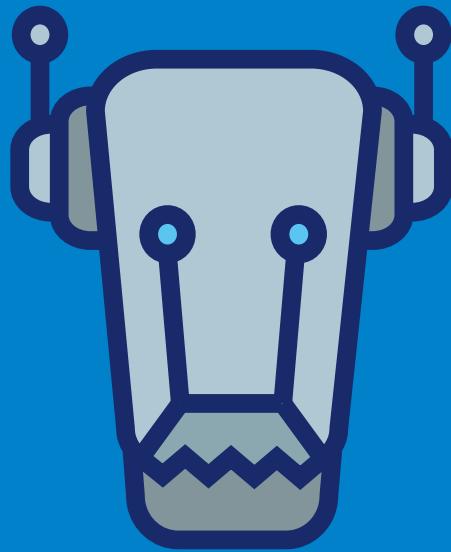
Physical



Nixu Cyber Rogues is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

RPA AGENT GONE BERSERK “BENDER” UNINTENTIONAL



11

nixu

RPA AGENT GONE BERSERK “BENDER”

Bender is a “Robotic Process Automation” agent implemented in-house by business people with no technical background and without proper testing. It has elevated permissions to several IT systems required for carrying out the tasks.

Motivation and goals

- Easy solutions for system integration
- Cutting corners
- Desire to avoid “IT projects”
- Lack of competence

Targets

- Misuse of permissions in all systems using RPA

Skills and methods

- Does not handle unexpected situations correctly
- Handles sensitive data insecurely and may leave it laying around
- Hasty solutions
- Misuse of extensive permissions

Resources and budget



\$\$\$\$\$

Harm potential



Accidental

Attacks from



From internet



Nearby



Nixu Cyber Bogies is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

ANNOYED USER “HYACINTH” INTENTIONAL



12

nixu

ANNOYED USER “HYACINTH”

Hyacinth is a consumer who is very conscious of regulations and her rights and will exercise these to the maximum. Hyacinth loves the small print and winning complex arguments. If Hyacinth gets annoyed about minor bugs or service faults, she doesn't hesitate to blame and shame publicly.

Motivation and goals

- Ideological reasons
- Revenge
- Irrational motives
- Winning an argument

Targets

- Public e-services
- Systems processing personal data
- Any information that supports her case

Skills and methods

- Simultaneous use of all customer communication channels
- Publishing information about faults and bad service in social media
- Calling yellow press about faulty service
- Extremely persistent

Resources and budget



Harm potential

● Abuse of functionality

Attacks from

● From internet



Nixu Cyber Bogies is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

BRUTAL CLEANER "SINI"

UNINTENTIONAL



13

nixu

BRUTAL CLEANER "SINI"

Sini is a cleaning specialist working on the premises. Sini is efficient and focused on the work and sees technology as physical objects that need to be cleaned or are in the way. Sini is not very technically oriented and may not understand the confidentiality of what she hears and sees.

Motivation and goals

- Efficiency – finish the cleaning job quickly
- Chats about things seen at work with friends

Targets

- Any physical objects in exposed spaces: cables, switches, buttons, touch screens
- Papers left on desks

Skills and methods

- While wiping dust off surfaces, pushes all buttons and swipes touch screens
- Unplugs power cables to get a socket for a vacuum cleaner
- Unplugs data cables when moving units
- Throws papers away from desks

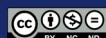
Resources and budget



Harm potential



Attacks from



Nixu Cyber Bogies is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

SOCIAL ENGINEERING VICTIM "PATSY" UNINTENTIONAL



14

nixu

SOCIAL ENGINEERING VICTIM "PATSY"

Patsy has worked at the company for fifteen years and has a lot of quiet knowledge. Patsy has extensive permissions and a "can-do" attitude, and is willing to help people outside their area of responsibility.

Motivation and goals

- Wants to help and get things done
- Avoid conflict
- Fear of authority

Targets

- Acquire sensitive information
- Get access to sensitive areas
- Cross an air gap with malware

Skills and methods

- Collaboration (e.g., help someone voluntarily with insider knowledge)
- Malware infection
- Spear phishing
- Malicious USB

Resources and budget



\$\$\$\$\$

Harm potential



Accidental

Attacks from



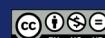
From internet



Nearby



Physical



Nixu Cyber Bogies is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

SUPPLY CHAIN ATTACKER “LISBETH” INTENTIONAL



15

nixu

SUPPLY CHAIN ATTACKER “LISBETH”

Lisbeth makes a living by sneaking backdoors and vulnerabilities into open source projects. Lisbeth is known for her advanced technical skills, which she uses to gigs that interest her. Sometimes she may be employed by the government, sometimes by an APT group.

Motivation and goals

- **Money:** Plant 0-day vulnerabilities that can be sold on the dark web or exploited by Lisbeth's employer

Targets

- Open source components developed with lax quality control
- Commercial integrations used by a large number of customers

Skills and methods

- Hides his tracks and obfuscates vulnerabilities
- **Supply chain attacks**
- Compromising part of the build and distribution infrastructure

Resources and budget



\$\$\$\$\$

Harm potential



Creates own exploits and tools

Attacks from



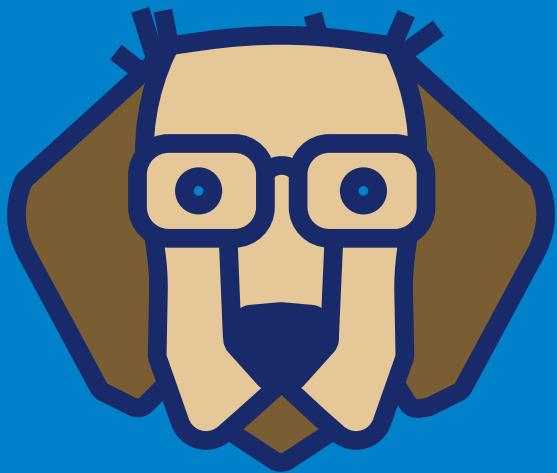
From internet



Nixu Cyber Bogies is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

INCOMPETENT DEVELOPER “DERK” UNINTENTIONAL



16

nixu

INCOMPETENT DEVELOPER “DERK”

Derk works in an advertising agency and does some web app coding in addition to UI design. Derk has no formal software engineering training and is not aware of common vulnerabilities, so he creates software with a combination of googling and a trial-error cycle. On top of regular working days, Derk does some night-time coding when the kids are asleep.

Motivation and goals

- Wants to contribute to the open-source community to get credit and to **have something on his CV**

Targets

- Users of open-source components
- Web and mobile application projects where Derk works

Skills and methods

- Copy-paste coding
- Injects all possible OWASP top 10 vulnerabilities accidentally

Resources and budget



\$\$\$\$\$

Harm potential



Accidental

Attacks from



From internet



Nearby



Nixu Cyber Bogies is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

THOUGHTLESS PROJECT MANAGER "AISHA" UNINTENTIONAL



17

nixu

THOUGHTLESS PROJECT MANAGER "AISHA"

Aisha is a project manager with a drive to go forward. She pushes her teams over their limits and gets projects done on time. Money comes first. Aisha makes decisions based on things she doesn't understand and is ignorant of security and privacy implications. Quality will be stripped off any enterprise system with a big price tag if Aisha is involved.

Motivation and goals

- Quick **money** and getting projects done on time – affects the personal bonus
- Not malicious – just does not understand technology

Targets

- Enterprise software systems
- SaaS software with custom-made integrations to client solutions
- Disruptive startups

Skills and methods

- **Ignorance**
- Not listening to subject matter experts
- **Hasty decisions**
- Pushing people to do their job quickly
- **Micromanaging**

Resources and budget



\$\$\$\$\$

Harm potential



Accidental

Attacks from



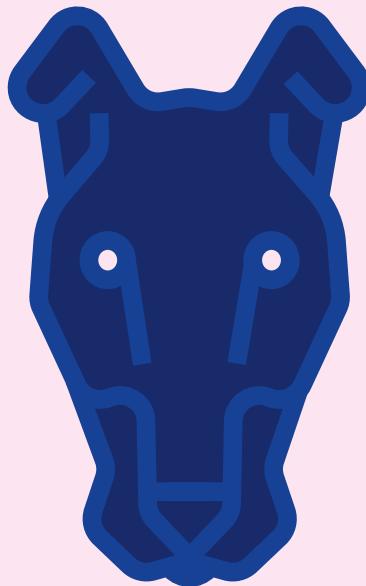
From internet



Nixu Cyber Bogies is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

ENTHUSIASTIC HACKTIVIST “ANONYMOUS N.N” INTENTIONAL



18

nixu

ENTHUSIASTIC HACKTIVIST “ANONYMOUS N.N”

Hacks for a cause to support ideological or political reasons.

“We are Anonymous. We are the Legion. Expect us.”

Motivation and goals

- Civil disobedience by digital means
- Remove control and capitalism
- Support freedom of speech, freedom of information flow and human rights
- May be politically influenced

Targets

- Websites
- IoT cameras and CCTVs
- Systems capable of causing damage: control systems
- Authorities' systems

Skills and methods

- DDoS attacks and threatening with a ransom
- Using ready-made attacking tools and exploits
- Simple web exploits
- Defacing sites

Resources and budget



Harm potential

- key Abuse of functionality
- cd Using ready-made tools

Attacks from

- globe From internet
- cross Physical



Nixu Cyber Rogues is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

ATTENTION JUNKIE “JULES” UNINTENTIONAL



19

nixu

ATTENTION JUNKIE “JULES”

Jules is a social media enthusiast who shares personal details openly on multiple social media platforms. Sometimes unintended content is visible. Jules is completely privacy-ignorant and is too impatient to read any user guidance.

Motivation and goals

- Gain fame and followers
- Share every minute and detail of their life. Online almost 24/7, also while at work
- Ignorance and impatience

Targets

- Websites and mobile applications asking for personal data, images, and videos
- Social media
- Data that ends up on the shared material

Skills and methods

- Click “Yes” to anything
- Never uses privacy settings
- Sharing without checking
- Ignorant exposure of others’ data

Resources and budget



\$\$\$\$\$

Harm potential



Accidental



Abuse of functionality



From internet

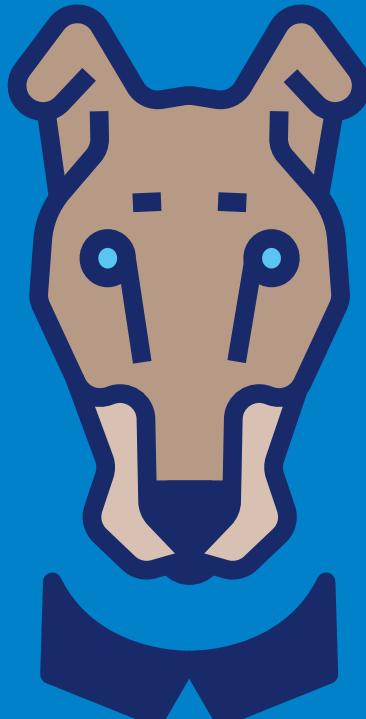
Attacks from



Nixu Cyber Bogies is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

CURIOUS GOSSIPER “GLENN” UNINTENTIONAL



20

nixu

CURIOUS GOSSIPER “GLENN”

Glenn is a likable and chatty employee who gets access to customer data and their sensitive information. During non-busy hours, Glenn takes a peek at the personal data of neighbors, colleagues, and celebrities for gossip.

Motivation and goals

- Unlimited **curiosity**
- Getting interesting information for coffee table **gossip**

Targets

- Customer support and issue handling systems
- CRM systems
- Sensitive records
- Anything with personal data

Skills and methods

- Gossip and social engineering
- Acts within their own access rights in the system
- Cannot cover their tracks

Resources and budget



Harm potential

钥 Abuse of functionality

Attacks from

- 🌐 From internet
- 📍 Nearby



Nixu Cyber Bogies is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

STUBBORN STALKER “SASHA” INTENTIONAL



21

nixu

STUBBORN STALKER “SASHA”

Sasha is obsessed with knowing what the ex-spouse does and where their kids are and what they do online. The smallest thing can trigger Sasha's obsession.

Motivation and goals

- Jealousy and obsession
- Feeling of control
- Revenge and causing any harm to the ex-spouse

Targets

- Ex-spouses and family members
- Famous people and celebrities
- Privacy and wellbeing
- Applications and devices (e.g., fitness tracking apps and smart devices)
- Unprotected devices and communication channels

Skills and methods

- Parental control applications
- Simple spyware
- Open-source intelligence in social media
- Social engineering passwords

Resources and budget



\$\$\$\$

Harm potential

- key Abuse of functionality
- cd Using ready-made tools

Attacks from

- locationNearby
- crossPhysical



Nixu Cyber Bogies is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

PROFITS FIRST MARKETEER “MO” INTENTIONAL



22

nixu

PROFITS FIRST MARKETEER “MO”

Mo wants to gather, track and link as much personal data as possible for profiling and marketing campaigns. Mo doesn't care about rules, ethics, or privacy laws.

Motivation and goals

- **Money:** Successful marketing campaigns
- **Reputation among colleagues:** Owning the most extensive and linked person databases
- Being a user behavior guru

Targets

- User processes
- Databases with personal data
- User interfaces
- User devices

Skills and methods

- Buying and selling of personal data
- Capturing data from processes
- Linking up data
- Tracking people where possible
- Access to databases

Resources and budget



Harm potential

钥 Abuse of functionality

Attacks from

- 🌐 From internet
- 📍 Nearby



Nixu Cyber Rogues is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

EVIL DATA SCIENTIST “AIDAN” INTENTIONAL



23

nixu

EVIL DATA SCIENTIST “AIDAN”

Aidan has a 6th sense when it comes to data analytics. Aidan sees linkability and relations, where others see only random data. Aidan analyzes data dumps and open data and sells the enriched data to those who don't care about ethics either.

Motivation and goals

- Money – selling enriched personal data sets
- Finding personal data of celebrities and famous people
- Likes the challenge of reidentification

Targets

- Open data APIs
- Data sets released for statistical purposes
- Data dumps from data breaches

Skills and methods

- Reversing weak anonymization
- Advanced data mining
- Correlating various data sources

Resources and budget



Harm potential



- Using ready-made tools
- Creates own exploits and tools

Attacks from



- From internet
- Nearby



Nixu Cyber Bogies is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu

DATA HAMSTER "HAYLEY"

UNINTENTIONAL



24

nixu

DATA HAMSTER "HAYLEY"

Hayley is a workaholic who needs all possible information to be able to work anytime, anywhere, even while on a beach holiday or on the airplane. Multiple copies and printed back-ups relieve Hayley's stress.

Motivation and goals

- Working anytime, anywhere
- Feeling of control
- The more data on hand, the better

Targets

- Sensitive records
- Classified material
- Investigation case files
- Government papers
- Digital and paper documents

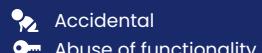
Skills and methods

- Export, download, copy and print
- Storing data on personal web services, portable media and all kinds of devices
- Making many copies

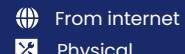
Resources and budget



Harm potential



Attacks from



Nixu Cyber Bogies is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc-nd/4.0/>.

nixu