

ReconOT

Global Attack Surface Mapping for Industrial Organizations

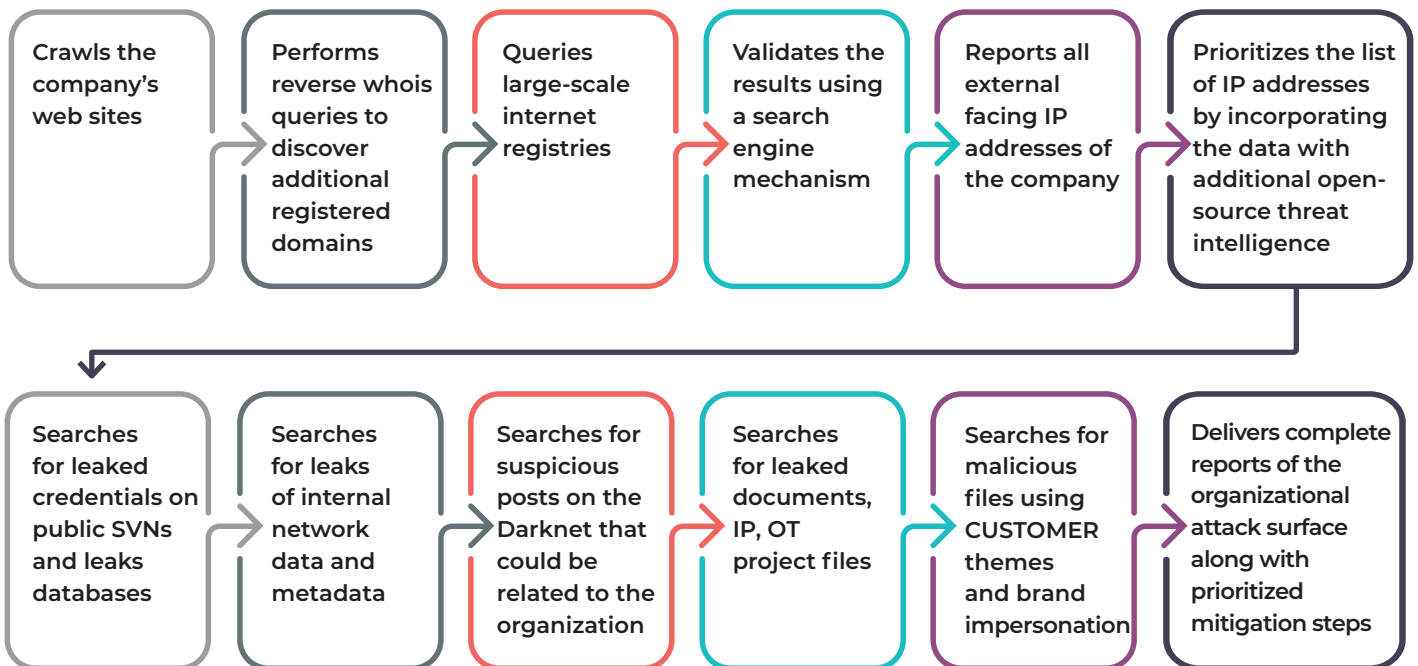
Combining OTORIO's ReconOT automated attack surface discovery tool with deep OT-cybersecurity intelligence and analysis

Using its proprietary ReconOT tool, OTORIO delivers a complete Global Attack Surface Mapping service for industrial organizations

ReconOT is an automatic, passive OT-centric reconnaissance tool for discovering a company's assets as they are seen by a potential attacker. The main purpose of ReconOT is to map all Internet facing services provided by a company, without triggering any alerts on the company's SOC / Blue team.

ReconOT provides a list of IP addresses connected to the company, prioritized by ease of discovery the complexity of the service's exploitation and the severity of the potential impact. The tool runs with zero impact on the services themselves and requires no preparation by the Customer's IT/Security team.

ReconOT Flow:

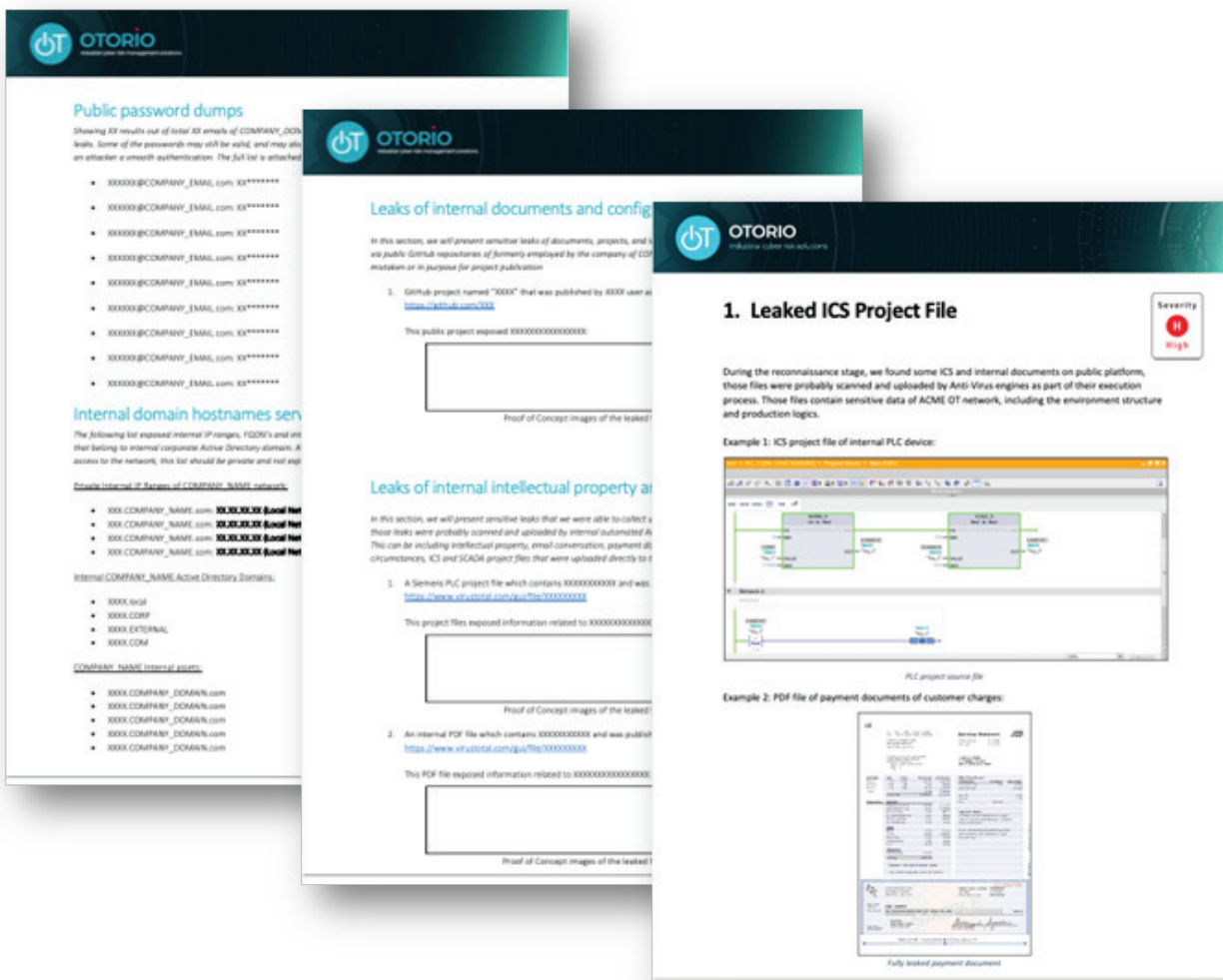


ReconOT advantages for Industrial Organizations

ReconOT focuses on the industrial market and OT aspects, unlike other attack surface tools that mainly focus on IT. ReconOT searches for OT related artifacts, such as leaked engineering stations project files and leverages an up-to-date database of leaks from the Darknet. Taking advantage of OTORIO's years of OT-security experience, ReconOT leverages unique methodologies of exposure of sensitive data in public source control.

With ReconOT, OTORIO delivers detailed reports that are backed and reviewed by professional industry veterans who fine tune the findings, provide context, and prioritize the required mitigation steps.

Sample Reports



Public password dumps
Showing 12 results out of total 12 emails of COMPANY_NAME leaks. Some of the passwords may still be valid, and may still be used for authentication. The full list is attached.

- XXXXX@COMPANY_EMAIL.com: XX*****
- XXXXX@COMPANY_EMAIL.com: XX*****
- XXXXX@COMPANY_EMAIL.com: XX*****
- XXXXX@COMPANY_EMAIL.com: XX*****
- XXXXX@COMPANY_EMAIL.com: XX*****
- XXXXX@COMPANY_EMAIL.com: XX*****
- XXXXX@COMPANY_EMAIL.com: XX*****
- XXXXX@COMPANY_EMAIL.com: XX*****
- XXXXX@COMPANY_EMAIL.com: XX*****

Internal domain hostnames seen
The following list exposed internal IP ranges, FQDNs and all that belong to internal corporate Active Directory domains. It applies to the network, this list should be private and not exposed.

Leaks of internal documents and config
In this section, we will present sensitive leaks of documents, projects, and all public GitHub repositories of formerly employed by the company of COMPANY_NAME or in purpose for project publication.

- GitHub project named "XXXX" that was published by XXXX user at <https://github.com/XXXX>.
This public project exposed XXXXXXXXXXXXXXXX.
Proof of Concept images of the leaked:

Leaks of internal intellectual property
In this section, we will present sensitive leaks that we were able to collect. These leaks were probably scanned and uploaded by internal automated AI. This can be including intellectual property, email conversation, payment documents, ICS and SCADA project files that were uploaded directly to GitHub.

- A Siemens PLC project file which contains XXXXXXXXXXXXXXX and was published on <https://www.stuxnet.com/gigafile/XXXXXXXXXXXX>.
This project files exposed information related to XXXXXXXXXXXXXXX.
Proof of Concept images of the leaked:
- An internal PDF file which contains XXXXXXXXXXXXXXX and was published on <https://www.stuxnet.com/gigafile/XXXXXXXXXXXX>.
This PDF file exposed information related to XXXXXXXXXXXXXXX.
Proof of Concept images of the leaked:

1. Leaked ICS Project File Severity: High

During the reconnaissance stage, we found some ICS and internal documents on public platform, these files were probably scanned and uploaded by Anti-Virus engines as part of their execution process. Those files contain sensitive data of ADME OT network, including the environment structure and production logics.

Example 1: ICS project file of internal PLC device:

PLC project source file

Example 2: PDF file of payment documents of customer charges:

Fully leaked payment document

About OTORIO

OTORIO delivers next-generation OT security and digital risk management solutions that ensure reliable, safe and efficient industrial digitalization. The company combines the professional experience of top nation-state industrial cybersecurity experts with cutting edge digital risk management technology to provide the highest level of protection to the critical infrastructure and manufacturing industry.