GOVERNMENTS' INCREASING DEPENDENCY ON INTERCONNECTED DIGITAL AND CYBER-PHYSICAL SYSTEMS MAKE THEM MORE AND MORE VULNERABLE TO CYBERATTACKS. IT IS NOT FOR NOTHING THAT THE DIGITAL WORLD IS ONE OF THE DOMAINS OF OPERATION.

HOWEVER, IF WE ACCEPT THAT CYBERSPACE PLAYS SUCH A SIGNIFICANT ROLE IN MODERN NATIONAL SECURITY, IT IS ALSO IMPORTANT TO KNOW WHAT WEAPONS ARE USED ON THIS BATTLEFIELD.

IN THE MAJORITY OF CASES, INTRUDERS DEPLOY MALWARE TO COMPROMISE CRITICAL ASSETS, ACQUIRE PERSISTENCE. MALICIOUS ACTORS INCLUDE GOVERNMENT-SPONSORED ORGANIZATIONS WITH DIVERSE GEOPOLITICAL BACKGROUNDS.

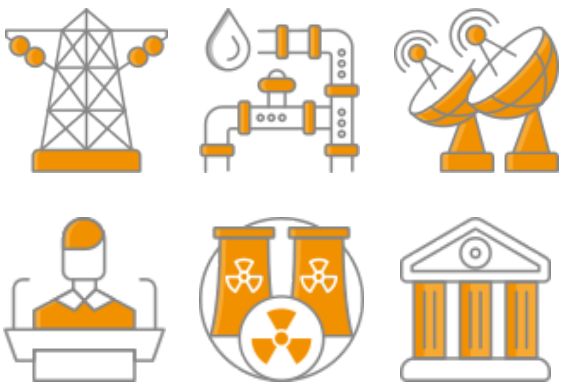
kaibou

Malware has a much shorter development time and a much higher dissemination rate than traditional weapons, but its impact can be just as great. The knowledge of malicious digital programs and the ability to defend against them is as important as any other aspect of national security.

Defense against malware is somewhat problematic:

1. The sheer volume and variety of malware today makes it almost impossible to track every attack.
2. Users think traditional antivirus programs are enough. Surely these programs do immense work, but even so, there is no further malware analytics / investigation. Sometimes dangerous attacks get through the leaks / fly under the radar.
3. Many modern malware are prepared for being analysed and are able to alter their behavior accordingly, making it more difficult to track them.

By compromising critical infrastructure and other functions under the jurisdiction of states, these organisations will be vulnerable. A responsible organisation in any nation's security cannot rely solely on IT partners, they have to develop their own defense capabilities, upgrade their own security postures.



Ukatemi's Kaibou products and complementary services provide a flexible yet firm solution.

UKATEMI TECHNOLOGIES

Kaibou LAB

Have you ever wanted to perform all the malware analysis tasks in-house? Kaibou Lab is a malware analysis laboratory that enables skilled experts to detect, discover and analyze malware in a completely safe sandbox environment, including the behaviour and impact of such attacks. This architecture supports the whole workflow: from sample classification through reporting to structured data storage.

Unique features:

- **modular and scalable architecture**
- **support for parallel analysis**
- **completely safe environment**
- **isolated workflows**
- **support for analyzing mobile IT platforms (iOS and Android)**
- **multiple antivirus prechecks with automated database updates**
- **full control of network access of the malware with easy firewall mgmt**
- **analysis workflow orchestrator**
- **pre-installed toolcase**
- **based on real life use cases**
- **support for collaborative reporting**
- **audit trail**

It contains various hardware components (including the analyst workstations, the back-end infrastructure storing data and the network infrastructure), software elements (including analyzer software and the software components required for system configuration) and interfaces both on network, service and application layers. Kaibou Lab supports workflows such as unpacking and de-obfuscation malware samples and artifacts, static and dynamic program analysis, creating reports.

Hardware Environment*

1. Virtualisation environment - at least 8 core processor, 4x16 GB memory, 4x4 TB storage
2. Knowledge base server - at least 8 core processor, 4x16 GB memory, 4x12 TB storage
3. Physical victim machines (x3) - at least 6 core processor, 8 GB memory, 256 GB storage
4. Physical workstations (x5) - at least 8 core processor, 16 GB DDR4 memory, 256 GB (internal hard disk) + 1TB (external removable hard disk) storage

Software Environment*

1. Analysis servers - VMware ESXi, vSphere hypervisor
2. Sandbox environment - Cuckoo Sandbox, VMs with pre-installed typical office applications, analysis apps and tools, a variety of antivirus software
3. Support servers: Ubuntu Linux; Debian Linux servers

Analysis tools*

Tools supporting coding /decoding; file extraction; file, program and network analysis; disassembling; decompiling; debugging; disc and memory forensics; etc.

Kaibou REPO

Kaibou Repo is a distributed malware database system designed to support malware analysis and threat intelligence services. The architecture of this repository is based on an extensible Hadoop cluster that enables further scalability. Incorporated intelligent storage solutions deliver high fault tolerance and reduce storage needs. Kaibou Repo offers multiple search options including search based on sample hash, sample similarity (TLSH) and yara rules - so when an attack occurs, you won't lose valuable moments.

- 470.000.000+ malware samples
- 700 TB data (with fault tolerance)
- continuously updated
- at least 2 years of malware feed (or as requested)

Features

- scalable system that can be expanded to match specific user needs: storage space, computational power, search speed
- low latency search in analysis results
- easy definition of new malware analysis tasks based on Yara
- low latency similarity search
- flexible, full-featured programmable API that enables integration of KAIBOU to other systems
- graphical interface for malware analysts

Hardware Environment*

Kaibou comprises of 10 or more server nodes, each of which deliveres large amounts of storage and computational power. Minimum hardware specifications of each node (can be altered based on user requirements):

- Processor: Intel or AMD, at least 8 cores, at least 4GHz turbo frequency
- Memory: at least 16GB
- Storage: sum above 48 TB

Software Environment*

Kaibou is based on Hadoop project extended with components developed by Ukatemi. Each node is delivered with stable Linux distribution installed (E.G. Debian, Ubuntu).
Software packages that are available in the final distribution of the OS will be pre-installed upon request.

*The parameters listed are indicative. The final hardware and software list included in the price will be adapted to the customer's needs and established in agreement with the customer.

kaibou

Training and consulting

We provide education to utilize each tool, with a rich list of use cases and best practices. The primary objective of our training is to train the malware analysts of the future within a couple of weeks. We have experience in educating experts on different levels - whether they come from the management or have more advanced technological background.

Our courses cover the most deadly malware attacks in history, nationwide malware exposure, android malware analysis, digital forensics, how and what technologies can be used to find malware (in memory, registry, etc.), classic reverse engineering tools and methodologies. Of course, each training and consulting session is altered to the unique needs of our clients.

About us

Ukatemi Technologies is a professional engineering company with demonstrated expertise and experience in high quality and unique cybersecurity services. We provide services and products to detect and prevent targeted cyber attacks: security design review, malware analysis, security posture evaluation and upgrade in both IT and OT environments, incident management and forensics after an attack.

Our experts hold a top secret site security clearance, and have been involved in the detection and analysis of several highly publicised targeted malware attacks (including Duqu, Flame, MiniDuke, TeamSpy). They also have experience in management of large-scale incidents, security assessment of critical information infrastructures, testing of anti-APT tools (BabO), vulnerability assessment of cyber-physical systems, development of risk analysis and security assessment procedures.