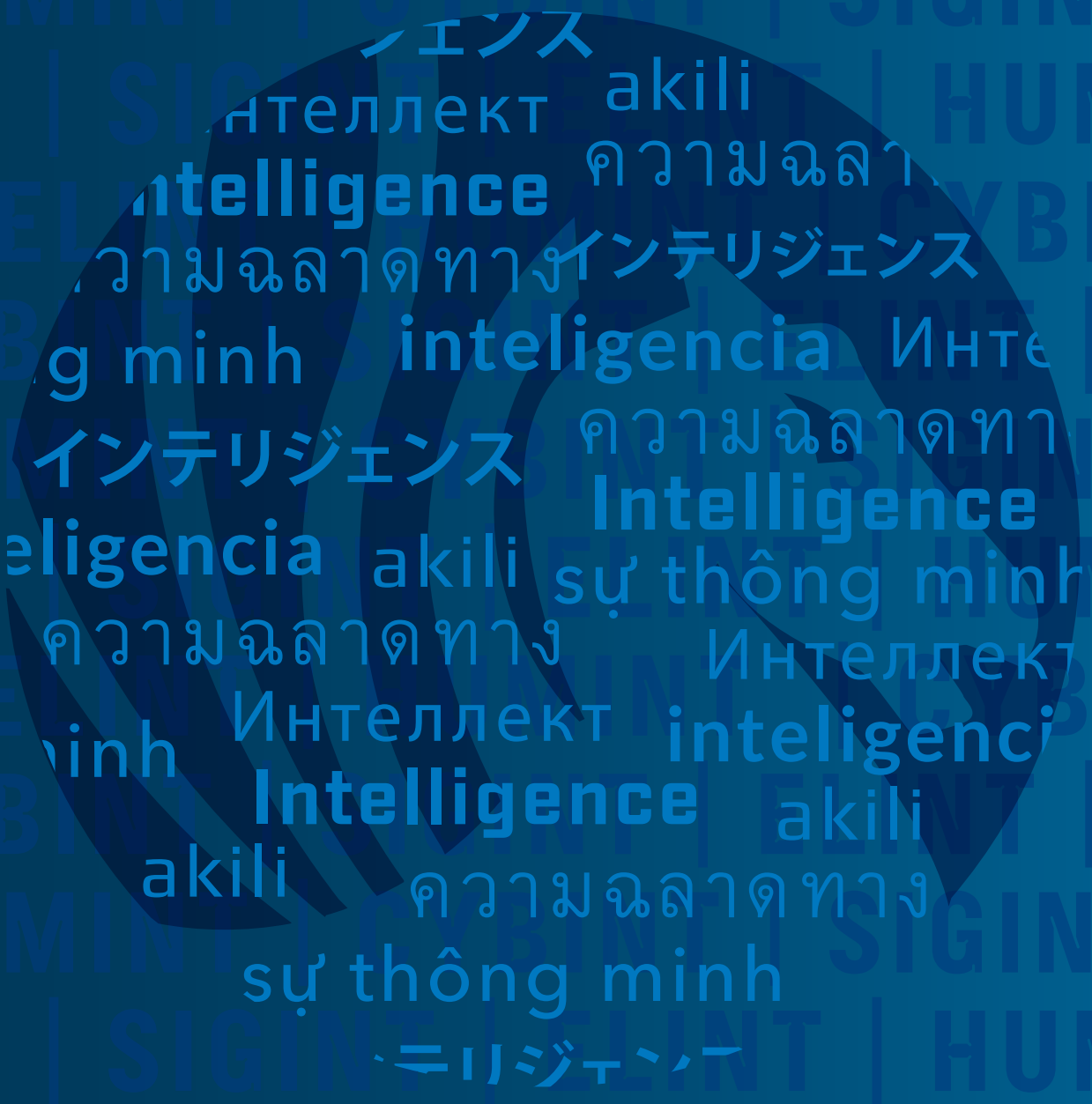
CYBINT



PEGASUS INTELLIGENCE 2016

DIGITAL NETWORK INTELLIGENCE GATHERED FROM CYBER SPACE

TABLE OF CONTENTS

PEGASUS

CYBER INTEL

GATHERING INFORMATION FROM TARGET'S COMPUTER OR PHONE (ANDROID AND IPHONE)

The only information needed for the service: email address to be investigated.

Pegasus service provides: Email content with history backlog or content of Hard disk.
Each email with history backlog: XXXXX Results on the flash disk (or computer not connected to Internet)

NOTE: In some difficult cases the price might be higher and this is discussed with the customer
Analysis of the received data can be provided.

Hard Disk Copy XXXXX and up depending on the case.

Prepay: 50%K USD
If no results received within 40 days – the deposit will be returned.
Service for remote transfer of the phone content: XXXXX
Updates: can be performed weekly. XXXXX

Requirements
1. Email address configured on the cell phone
2. Phone model and number (desirable)

DATA SUPPLIED FROM THE TELEPHONE

iPhones

1. Call Details- calls history feature: call logs containing details of incoming and outgoing calls, which includes date, time and duration of the calls.
2. Browser History Logging- view all webpages viewed by the target person.
3. Contact Details- View the all contact details saved on the iPhone.
4. Location Tracking- monitor every movement automatically at a predefined interval.
5. WhatsApp Chat Logging- WhatsApp logging ability which enables you to view all sent and received WhatsApp messages.
6. Email Logging- View all the details of sent and received emails.
7. Picture & Video Logging- all the pictures and videos stored on phone has been uploaded.
8. Text Message Logging- SMS logging ability which enables you to remotely view all sent and received text messages of target iPhone.

Android

1. Application List- This feature allows you to view details of all apps installed on phone
2. Video Logging- view all videos on the Android phone you are tracking
3. Text Message Logging- view all details of text messages
4. Web History- tracks the entire web browsing
5. Picture Logging- logs all pictures on Android phone being tracked.
6. GPS Tracking- continuously tracks the subject even when traditional GPS tracking fails
7. Contact Details- view the details of contacts—even masked ones!
8. Call Details- view complete call log of every call made or received

PEGASUS

BLACK BOX DDOS

DISTRIBUTED DENIAL OF SERVICE ATTACK SYSTEM

A denial of service (DOS) attack is a malicious attempt to make a server or a network of resource unavailable to the users, usually by temporarily interrupting or suspending the services of a host connected to the internet.

DOS attacks are implemented by either forcing the targeted Servers to reset, or consuming its resources so that it can no longer provide it's intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

Until now performing effective DDoS attacks involved thousands of slave computers that generate a Traffic Overload and by this delaying and even blocking the availability to or from the web service or web server.

BLACK BOX

It is a stand-alone, server based system that is designed to perform an autonomic and independent Remote DDoS attack over the internet/network based services such as;

INTERNET WEB SITE

Banks

Cellular Providers

News Web Sites

Commercial Web Sites

Web Forums

Blogs

Dedicated News or article pages

Stock Market web sites

WEB SERVICES

Web Mail

Chat Servers

redit Card Payment Gateways

Root Name Servers

PEGASUS

BLACK BOX

PENETRATION TESTING

THE DANGER

Out of every 10 servers tested by Gold Lock, 40% end up with the security team being able to perform one or more of the following:

DENIAL OF SERVICE

Bring the system to a complete halt.

SPYING

Extract information such as DB tables, user passwords, confidential files...

CONTAMINATION

Modify websites and applications causing them to display and/or transmit specific data.
*Cases above are demonstrated with the owner's permission only and always with prior consultation.

DEFEATING HACKERS AT THEIR OWN GAME

Gold Lock evaluates the security of a computer system or network by simulating an attack from a malicious source (hacker).

The process involves an active analysis of the system from the position of a potential attacker for any potential vulnerability that could result from improper system configuration, outdated hardware or sofware, or operational weaknesses in process or technical countermeasures.

Any security issues that are found are confidentially presented to the system owner, together with an assessment of their impact, and with a detailed proposal for a quick resolution of the discovered breach.

The intent of a penetration test is to determine the feasibility of an attack and the amount potential damage of a successful exploit, if discovered.

ADVANTAGES

Trusted

Gold Line Group is an international leader in information security, its line of encryption products are trusted by security organizations all over the world, and its employees are military trained experts.

Secure

Testing is purely black box, Gold Lock's team of experts does not ask for any information about the target system, and works to retrieve information available for everyday hackers.

Confidential

Test results are kept strictly confidential, and are securely delivered to the customer only.
Constant: Periodical tests with clear action items for closing any security holes.

Global

Gold Line Group's worldwide presence guarantees that regardless of the size or location of your network, we will provide the security your organization needs.

ACSC

ADVANCED CYBER SECURITY CENTER

Gold Lock offers a unique approach for building a modern, state of the art, highly efficient advanced cyber security center (ACSC), utilizing the latest technology and methodologies available in the world of information security, while making sure to always improve and update it as times change.

NETWORK INTRUSION DETECTION SYSTEM (NIDS)

A sophisticated control center, working 24 X 7, enables ACSC teams to view all crucial networks together in real time, using specialized equipment and software, all network activity is monitored, constantly analyzed, and automatically compared to known patterns of attacks from around the world. Smart NIDS sensors alert ACSC teams on screen, by SMS, and by email whenever an attack is taking place, advising them of the exact location, making sure ACSC is never taken off guard.

Each attack/intrusion attempt is automatically logged and recorded for further analysis and optionally for taking offensive measures against the attackers later on.

DEPLOYING ENCRYPTION

One of the most important factors in cyber security is safeguarding secret information. Gold Lock specialists have the best understanding in the world on how that is done, an understanding stemming from many years of inventing and developing the world's most secure communication systems.

Gold Lock and ACSC teams will jointly deploy the highest level of encryption on servers, databases, personal computers, communication channels, and make use of advanced technologies such as smart cards to make sure information stays in the hands of

PENETRATION TESTING

DOS, Social engineering, cross-site-scripting, SQL Injections and thousands of attacks which are constantly invented present a day to day threat that can not be ignored. Gold Lock specialists know about all of them, and are responsible for keeping constantly updated about new ones. With their training, ACSC teams are able to perform these attacks on various servers, reviewing the results, and fixing vulnerabilities before other attackers gain access to crucial systems.

SPECIAL CYBER ATTACK UNIT

ACSC will form a specially trained assault team, highly proficient in all types of cyber attacks, enabling it form a significant deterrent against hackers, and other hostile entities. ACSC attack capabilities will constantly be updated to match those of the best hackers in the world, using a multitude of attacks to gain access, disable, penetrate and monitor target systems, servers, databases, mobile phones, GPS's and other communication channels.

SMART USE OF NEWEST TECHNOLOGIES

Keeping updated with the latest technology is Gold Lock's specialty. Gold Lock will work with ACSC teams to remain on the cutting edge of the security field, utilizing mainly open source security systems which are constantly updated by a global community counting tens of thousands of security professionals. Thus making the maximum out of ACSC's budget, enabling it to dedicate more resources to a multitude of crucial tasks.

TRAINING & EDUCATING

99% of all major cyber attacks could have been prevented by taking simple, not expensive means of defense beforehand. This is usually not done - because of apathy and lack of knowledge.
The most important pillar of the ACSC is implementing a system that promotes constant training and educating.
Training ACSC staff, keeping them current in all the latest advances in technology, new types of attacks, new methods of defence and offence.
Educating personnel responsible for crucial government infrastructure, information, equipment, thus helping them maintain their systems safe. And equally important - periodically reviewing their systems to make sure they stay safe.

SHARED INFORMATION

A key advantage of ACSC in staying ahead of hackers, is to maintain a shared DB of threats & solutions, which can be access by all authorized government personnel. The shared DB ensures smart cooperation and shared use of the latest security information, so when progress is achieved by a few people, it propagates to the rest of the chain automatically, causing the entire system to grow strong.

CONSTANT REVISION & UPDATE

Gold Lock's project managers constantly work with ACSC team leaders, creating procedures that promote constant revision and updates of the way we work. Our joint goal is to always improve, learning from past mistakes and making sure we do not repeat them.
Periodic evaluation sessions will be conducted, briefing all medium and major security incidents, analyzing them, and implementing measures that makes ACSC safer, more efficient, and more powerful.