Duqu, Flame, Gauss: Followers of Stuxnet

Boldizsár Bencsáth Phd

BME CrySyS Lab

http://www.crysys.hu/

Session ID: BR-208

Session Classification: Advanced

The Story Begins with Stuxnet (June 2010)

- “the Most Menacing Malware in History” (Kim Zetter, Wired)
- targeted the Natanz nuclear enrichment plant in Iran
- modified PLCs (Programmable Logic Controllers)
- destroyed hundreds of uranium centrifuges

The DUQU malware

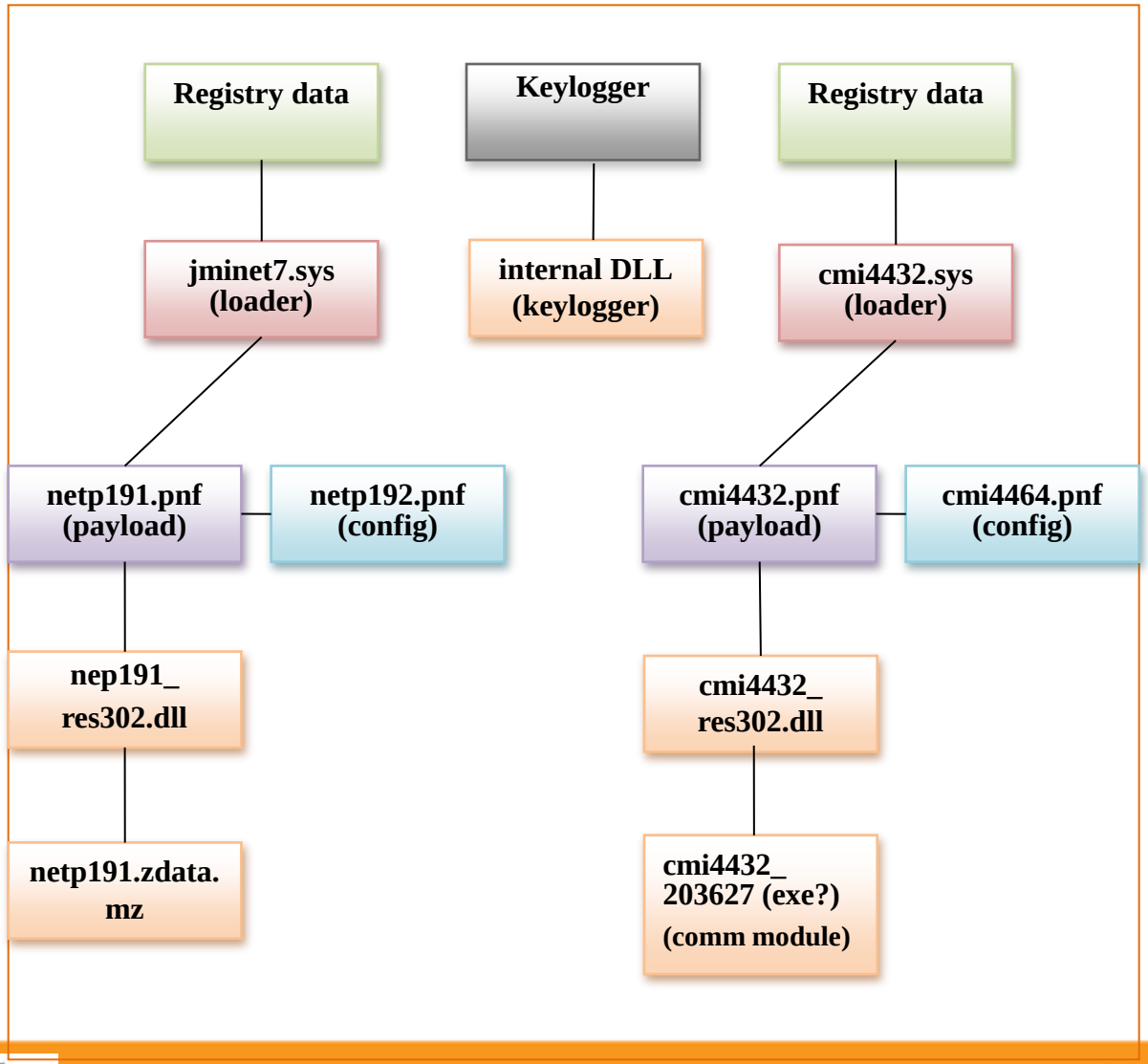
Duqu

- Duqu is a malware that **we discovered** in the wild in an incident response investigation
- Stuxnet: self-replicating malware to harm Iran's uranium enrichment centrifuges
- Duqu: information gathering
- Naming: infostealer component creates files starting with the string **"~DQ"**
- Duqu = Stuxnet ?
  - striking similarity in terms of design philosophy, internal structure and mechanisms, implementation details, and the estimated amount of effort needed to create it

Duqu (October 2011)

- striking similarity to Stuxnet
  - design philosophy
  - internal structure and mechanisms
  - implementation details
  - **digitally signed driver**
  - estimated amount of effort needed to create it
- completely different objective, though
  - steals information (key strokes, screen shots, files)
- ~20 known victims, including some in Europe

Duqu Components Found at CrySyS Case



Hungarian Lab found Stuxnet-like Duqu malware

By Ryan Naraine | October 21, 2011, 9:11am PDT

Summary: *The Laboratory of Cryptography and System Security (CrySyS) in Hungary confirmed its participation in the initial discovery of the Duqu cyber-surveillance Trojan.*

A security lab attached to the Budapest University of Technology and Economics in Hungary has come forward as the mystery outfit that found the Stuxnet-like "Duqu" cyber-surveillance Trojan.

According to Symantec's initial report on Duqu [PDF], the malware sample was passed along by an unnamed "research lab with strong international connections," a statement that led to speculation about the origins and intent of the threat.

Our contributions to Duqu investigations

- **discovery, naming, and first analysis of Duqu**
  - info-stealer component creates files with a name starting with ~DQ
  - our analysis focused on showing the similarities to Stuxnet
  - we shared our report with major anti-virus vendors and Microsoft
- **identification of the dropper**
  - MS Word document with a 0-day Windows kernel exploit
  - we shared the anonymized dropper with Microsoft
  - first patch in December 2011, further patches in May 2012
- **development of the Duqu Detector Toolkit**
  - focus on heuristic anomaly detection
  - detects live Duqu instances and remains of earlier infections
  - also detects Stuxnet
  - open-source distribution (to be used in critical infrastructures)
  - 12000+ downloads from 150 countries

Press coverage…

Hungarian Lab found Stuxnet-like Duqu malware

By Ryan Naraine | October 21, 2011, 9:11am PDT

Summary: The Laboratory of Cryptography and System Security (CrySyS) in Hungary confirmed its participation in the initial discovery of the Duqu cyber-surveillance Trojan.

Researchers discover zero-day Windows exploit in Duqu virus

The Duqu virus uses a previously unknown vulnerability to hijack Window's …

by **Sean Gallagher** - Nov 2 2011, 4:13pm CEST

Open-source Duqu detector toolkit released

By Ryan Naraine | November 10, 2011, 1:09am PST

Summary: The Laboratory of Cryptography and System Security (CrySyS) in Hungary has released an open-source toolkit that can find traces of Duqu infections on computer networks.

…And Professional Reputation

Symantec. | Conn

COMMUNITY: Security

Duqu Status Updat

Updated: 24 Oct 2011 | Translations avai

Symantec Security Respo

Symantec. | Official Blog

As mentioned in our previous blog investigating a targeted attack on Cryptography and System Securit Technology and Economics. CryS stated that no data was leaked as

We are grateful to CrySyS—shari determined that the originally targ the industrial infrastructure industi http://www.crysys.hu/.

The latest version of our white pap being downloaded onto a compror information comes to light.

Enter keywords to search...

The Mystery of Duqu: Part Two

0.7

Aleks
Kaspersky Lab Expert
Posted October 25, 19:59 GMT
Tags: Rootkits, Targeted Attacks, Industrial control systems, Stuxnet, Certificate authorities

Our investigation and research of Duqu malware continues. In our previous report, we made two points:

- there are more drivers than it was previously thought;
- it is possible that there are additional modules.

Besides those key points, we concluded that unlike the massive Stuxnet infections, Duqu attacks are limited to an extremely small number of targets.

But before informing you about our new findings, I would like to pay tribute to the Hungarian research laboratory Crysys for their work. They were the first who analyzed Duqu components and generated an excellent report. It was later provided to antivirus vendors and became the basis of further investigations.

(Unfortunately, our company was not the first to receive this report, but now it's even more interesting to find out everything about Duqu)

Our experts continue to conduct in-depth analysis of all Duqu components, and are finding more evidence of similarities between Duqu and Stuxnet. A detailed report with our experts' analysis of files and their structure is in progress and will be published later. This part of our research is not the most urgent. It is much more important to understand the details of the attacks and the facts, which will be discussed here.

Flame/Flamer/sKyWIper

Flame/Flamer/sKyWIper

- In May/2012 we participated in an international collaboration to investigate a novel malware, we called it sKyWIper
- 27/05 – National CERT of IRAN (MAHER) disclosed they are investigating a malware “Flamer”
- 28/05 – CrySyS released initial tech report on Flame/sKyWIper; Kaspersky released details about their work on “Flame”.
- We give no details what was exactly the collaboration, with whom we were working on and how.

Flame details

- Flame is possibly the most complex malware ever
- We produced an initial detailed analysis (~60 pages) of Flame with the help of others:

http://www.crysys.hu/skywiper/skywiper.pdf

- We wrote some blog entries on insights of Flame (USB storage, GPL license violation of Duqu, WuSetupV.exe URL creation

http://blog.crysys.hu/

- sKyWIper name is for ~KWI temporary files and the possible connection between “wiper” malware of Iran

Characteristics of Flame

- "most complex malware ever found" – main component is ~6MB
- another info-stealer malware
  - activates microphones and web cam
  - logs key strokes
  - takes screen shots
  - extracts geolocation data from images
  - sends and receives commands and data through Bluetooth
- data saved in SQL databases
- data transport via network connections and USB pen drive
- **infects computers by masquerading as a proxy for Windows update**
  - uses a fake certificate that looks like valid Microsoft certificate
  - needed advanced collision attack on the MD5 hash function
- thousands of victims, mostly in Iran and Middle East, but also in Hungary!

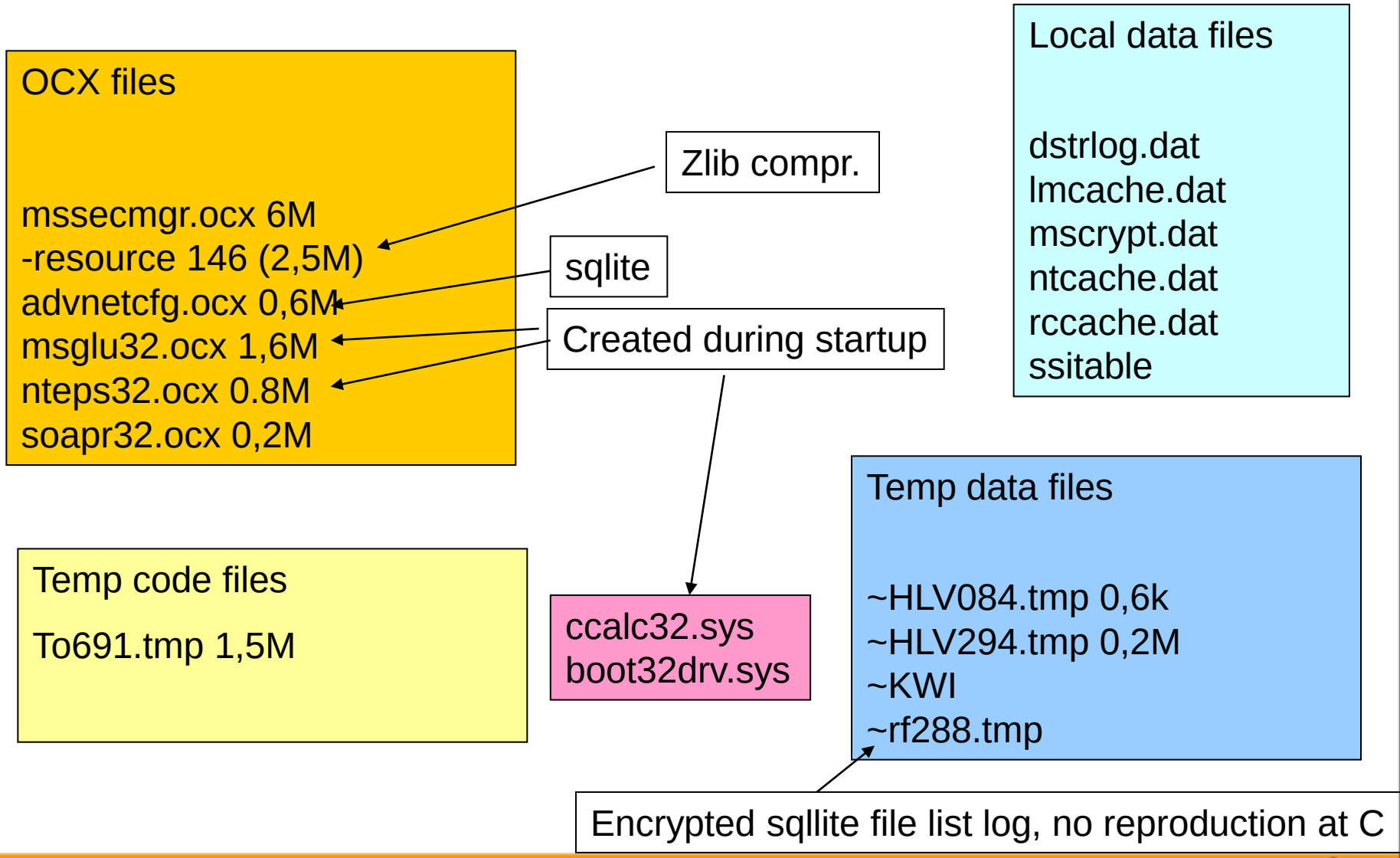
Comparison of Flame and Stuxnet/Duqu

Feature	Duqu, Stuxnet, ~D	sKyWIper
Modular malware	✓	✓
Kernel driver based rootkit	✓	fltmgr usage
Valid digital signature on driver	Realtek, JMicron, C-media	Not found
Injection based on A/V list	✓	Different
Imports based on checksum	✓	Not seen
3 Config files, all encrypted, etc.	✓	Totally diferrent
Keylogger module	✓ (Duqu)	✓
PLC functionality	✓ (Stuxnet)	Not found (yet)
Infection through local shares	✓ (Stuxnet)	✓ Very likely
Exploits	✓	✓ Some from Stuxnet!
0-day exploits	✓	Not yet found
DLL injection to system processes	✓	✓ (but different)
DLL with modules as resources	✓	✓
RPC communication	✓	?
RPC control in LAN	✓	?
RPC Based C&C	✓	?
Port 80/443, TLS based C&C	✓	SSL+SSH found
Special “magic” keys, e.g. 790522, AE	✓	Only 0xAE is similar
Virtual file based access to modules	✓	Not seen
Usage of LZO lib	Mod. LZO	No LZO: Zlib, PPMd, bzip2
Visual C++ payload	✓	✓
UPX compressed payload,	✓	some
Careful error handling	✓	?
Deactivation timer	✓	Self-kill logic inside
Initial Delay	? Some	Different from Duqu
Configurable starting in safe mode/dbg	✓	Not like Stuxnet

Flame and Duqu/Stuxnet Differs

- Flame is a platform different form Duqu (and Stuxnet)
  - larger code size
  - use of Lua scripting language
  - use of SQLite databases
  - larger C&C infrastructure
  - C&C servers run different OS (Ubuntu vs. CentOS Linux)
- they may be two implementations for the same requirement specification developed by two different teams
- the two teams may not be independent
  - Kaspersky researchers found chunks of code from a 2009 Stuxnet variant inside Flame

Flame Modules Found in First Round



Flame Related Files (partial)

preg.exe
ntcache.dat
lmcache.dat
rccache.dat
dcomm.dat
dmmsapi.dat
~dra52.tmp
commgr32
target.lnk
ccalc32.sys
~DEB13DE.tmp
zff042
urpd.ocx
Pcldrvx.ocx
~KWI
guninst32
~HLV
~DEB93D.tmp
lib.ocx
lss.ocx
~DEB83C.tmp
stamn32
~dra53.tmp
nteps32
cmutlcfg.ocx
~DFL983.tmp
~DF05AC8.tmp
~DFD85D3.tmp
~a29.tmp
dsmgr.ocx
~f28.tmp
desc.ini
fib32.bat
~d43a37b.tmp
~dfc855.tmp
Ef_trace.log
contents.btr
wrm3f0
scrcons.exe
Wavesup3.ocx
Ntep32.ocx
m4aaux.dat
mpgaud.dat
msaudio
mspbee32
~a49.tmp
wpgfilter.dat
Ssitable
urpd.ocx
lib.ocx
lss.ocx
target.lnk
stamn32

Our Contribution

- first detailed technical analysis of Flame (~60 pages) that became de facto standard reference in the community
  - identification and analysis of main modules, storage formats, encryption algorithms, injection mechanisms, activity in general
  - 65000+ downloads from 188 countries

An **in-depth look at Flame by the Laboratory of Cryptography and System Security** at Hungary's University of Technology and Economics in Budapest, said it stayed hidden because it was so different to the viruses, worms and trojans that most security programmes were designed to catch.

Gauss and others

Gauss

- Gauss is an information stealer malware based on the Flame platform – Found by Kaspersky Lab
  - injects its modules into different browsers in order to intercept user sessions and steal passwords, cookies and browser history
  - collects information about the computer's network connections
  - collects information about processes and folders
  - collects information about BIOS, CMOS RAM
  - collects information about local, network and removable drives
  - infects USB drives with a spy module in order to steal information from other computers
  - interacts with a command and control server, sends the information collected, downloads additional modules
- infections date back to September-October 2011
- thousands of victims, mainly in Lebanon, Israel, and the Palestinian Territory

Our Contribution on Gauss Story

- Gauss was discovered and analyzed by Kaspersky Lab
- in a very short time after the publication of the Kaspersky report, we provided an on-line Gauss Detector Service at gauss.crysys.hu
  - Gauss installs a font called Palida Narrow on victim computers
  - purpose is unknown (Paladin Arrow?)
  - our service checks the presence of the Palida Narrow font on client computers
- serving 85000+ requests, logged ~100 positives and notified them mainly in Lebanon and the US

The Gödel Module of Gauss

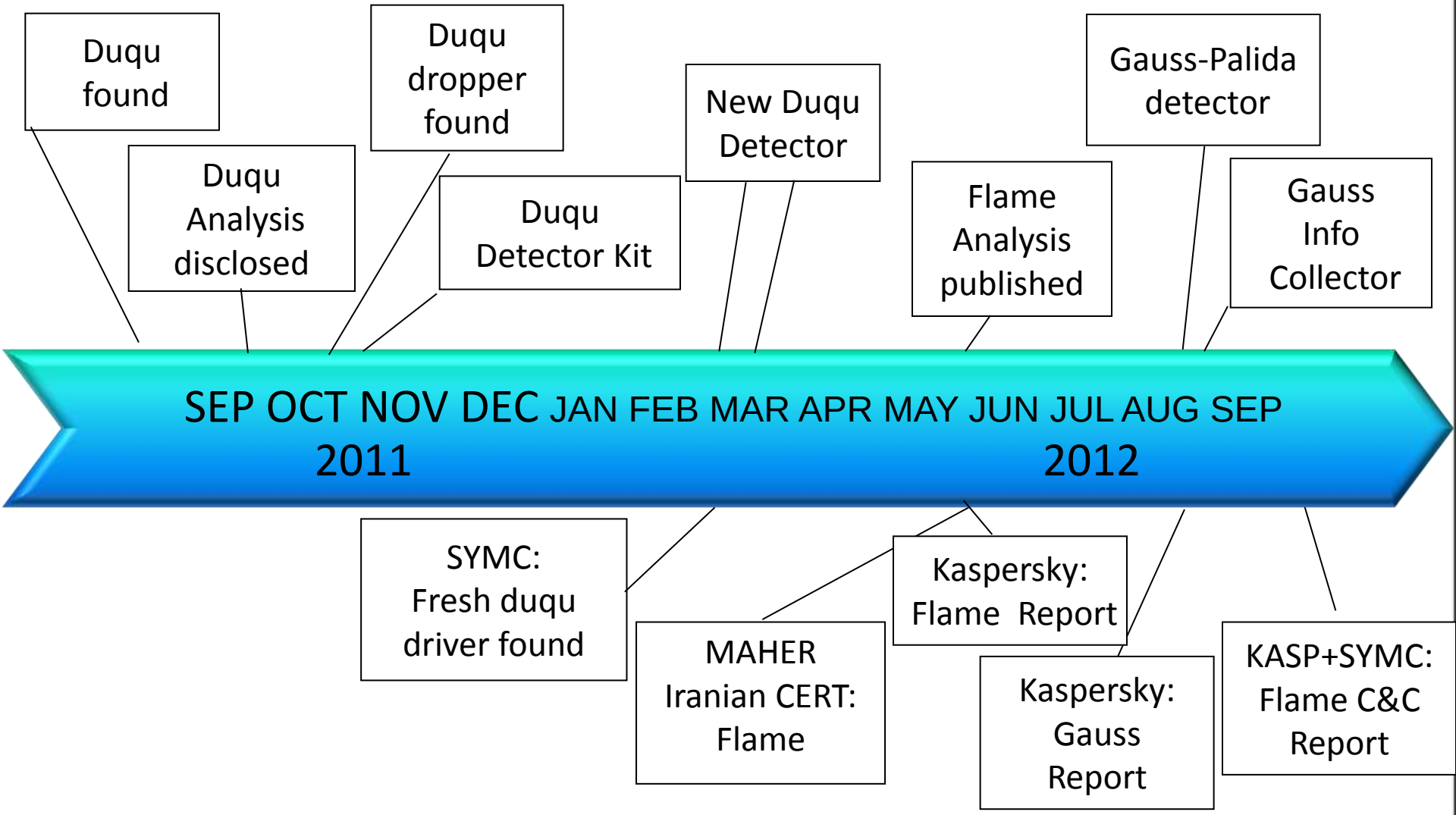
- Gauss' encrypted warhead
- unlike in case of Stuxnet, Duqu, and Flame
  - the encryption is not simple XOR masking or byte substitution
  - the decryption key is not available in the malware itself
- instead, Gauss uses RC4 and constructs the key dynamically from strings found on the victim system
  - this payload is executed only on the designated target system(s) that has the right configuration resulting in the correct decryption key
  - analysis of intent and functioning is made impossible for the research community
- the module is big enough to contain a Stuxnet-like SCADA targeted attack code and all the precautions used by the authors indicate that the target is indeed high profile
- We created a free tool „**Gauss Info Collector**" to collect PATH and Program Files directory information from volunteers

Discussion

Most Interesting Novelties of Recent Targeted Malware

- Stuxnet PLC module
  - Injecting code into PLC and destroying uranium centrifuges is really fascinating
- Stolen keys for signing drivers for Stuxnet (2 pieces) and Duqu (1)
  - It is not usual to steal code signing keys for creating efficient malware
- Duqu Windows kernel TTF exploit (CVE-2011-3402)
  - Gaining kernel level access with exploits is rare, especially in such a complicated manner
- Flame MD5 collision and Windows Update based propagation
  - Possibly cryptographic breakthrough was needed and/or exceptional computational resources to create fake certificate by collision attack
- Gauss Gödel module: encrypted payload which can be decrypted only on target
  - Researchers also proposed the idea which is now in the wild: payload is only decryptable if proper PATH and „Program Files” contents are available: just on the target

Timeline of CrySyS Lab Work of the Last Year on Targeted Malware



Malware Families at a Glance

- Stuxnet, Duqu, Duqu modules + Wiper?
  - At least the platform is created by same group.
  - Complex,clean code, well tested.
  - Only minimal part is delivered on victim file system.
  - Uses different C&C for each target -> very hard to discover
  - Duqu: Self-cleaning (suicide) after limited time -> to remain undetected
- Gauss and Flame, SP, SPE, … +Wiper?
  - The code is much sloppier, bunch of code put together (possibly lack of cleanup garbage, unused code too)
  - Debug and similar information left widely in code helping analysis
  - High level code like LUA scripts, SQLite database, etc.
  - Most modules delivered to targets, and there are lots of targets
  - Huge C&C server infrastructure (35+ servers)
  - **Flame C&C support three other malware: SP, SPE, IP**
- Shamoon
  - Likely not related to the above two
  - Amateurish errors
  - Major goal: wiping, but possibly also to obtain information
  - From operation point of view, very hard to judge who is behind (targets: oil industry in Saudi Arabia, Qatar)

Management and Mediator Role

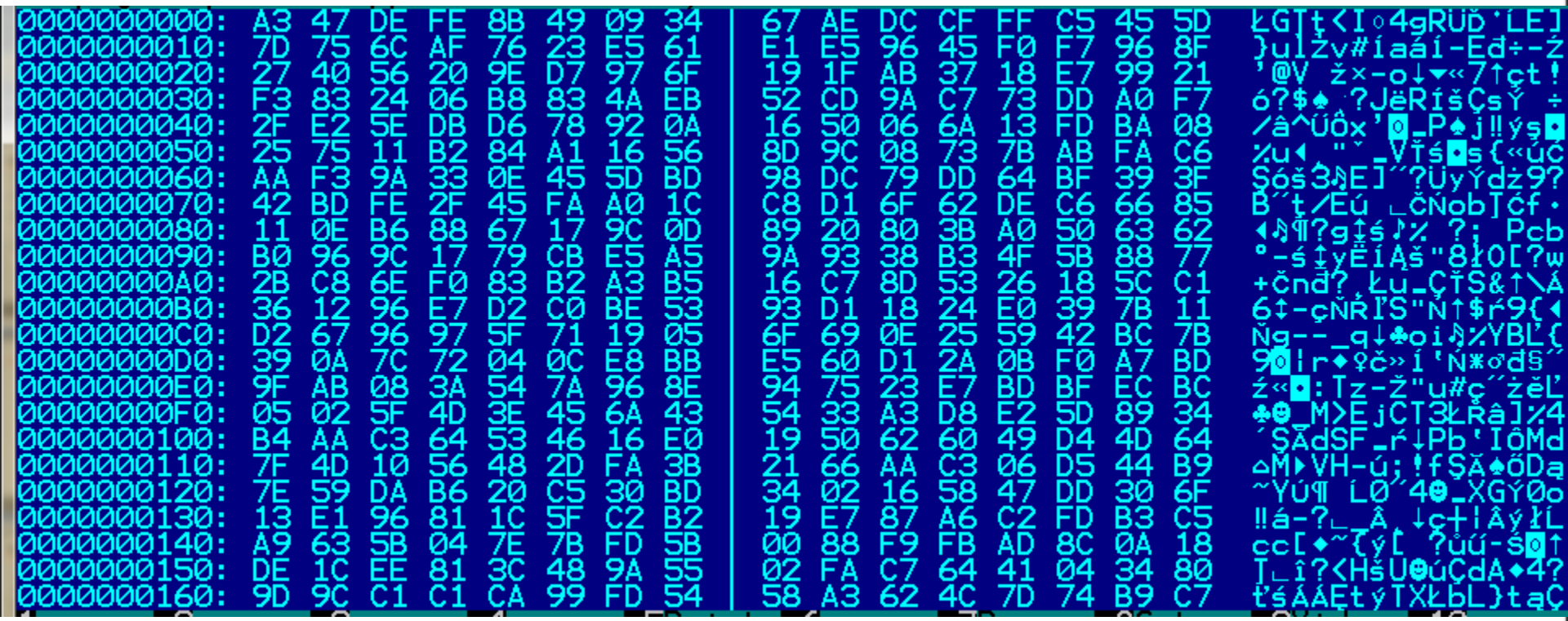
- 70-80% of our work is non-technical, much of that is after disclosure
  - What to tell, share, disclose
  - What not to tell, share or disclose
  - What permissions needed
  - Obtaining legitimate contact points to partners
  - Checking identity (legitimity) of parties
  - Encryption related problems (key exchange, key check etc)
  - Checking press, twitter, webinars, etc. to keep up with the world
  - Selecting, saving important information found on the net

Info sharing problems

- Duqu: Code/sample cannot be shared until proved that no data related victim is in the sample
- Flame: Sample cannot be shared in full depth as it can contain sensitive/victim related information
- Both: Even if the malware had victims in Europe, it is still a question if, or when public disclosure of information should be done
- Duqu: Company wanted to remain anonymous
  - We had to have our report published as anonymous appendix of Symantec report
  - Many newspapers stated Symantec found Duqu
  - Reputation/trust is more important than publicity

Calc32.sys of flame

- Obviously it's encrypted
- But what it is, should I share?

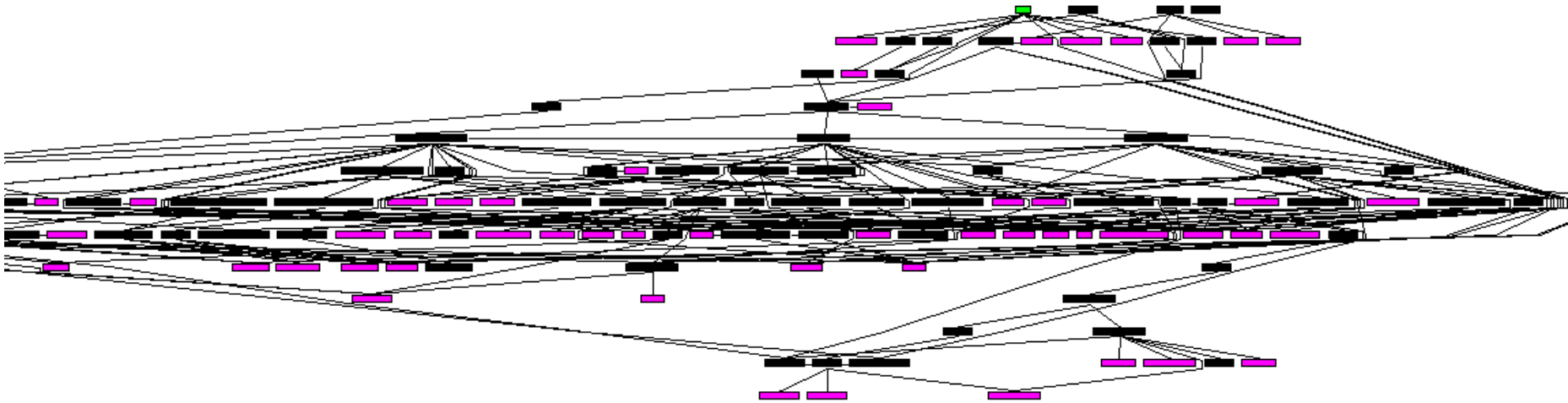


Calc32.sys after decryption

- It's not executable, but data
- Maybe it contains target specific values
- Sharing is problematic

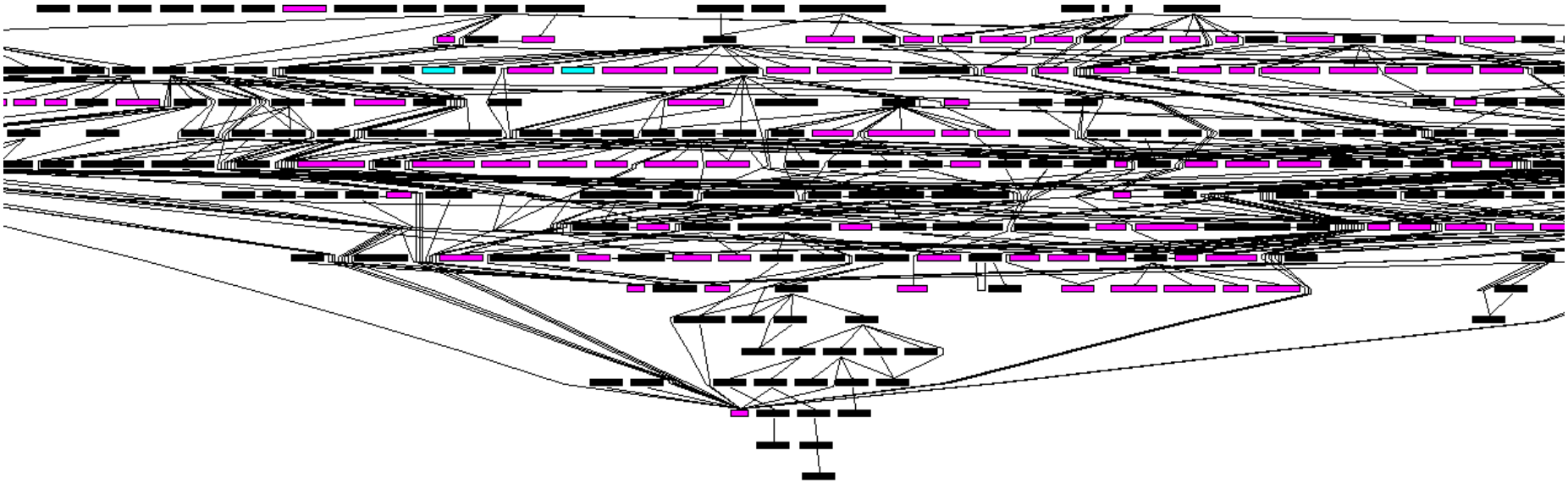
Structure of WuSetupV/Flame

- Took some weeks to get someone disclose details on its URL creation mechanism



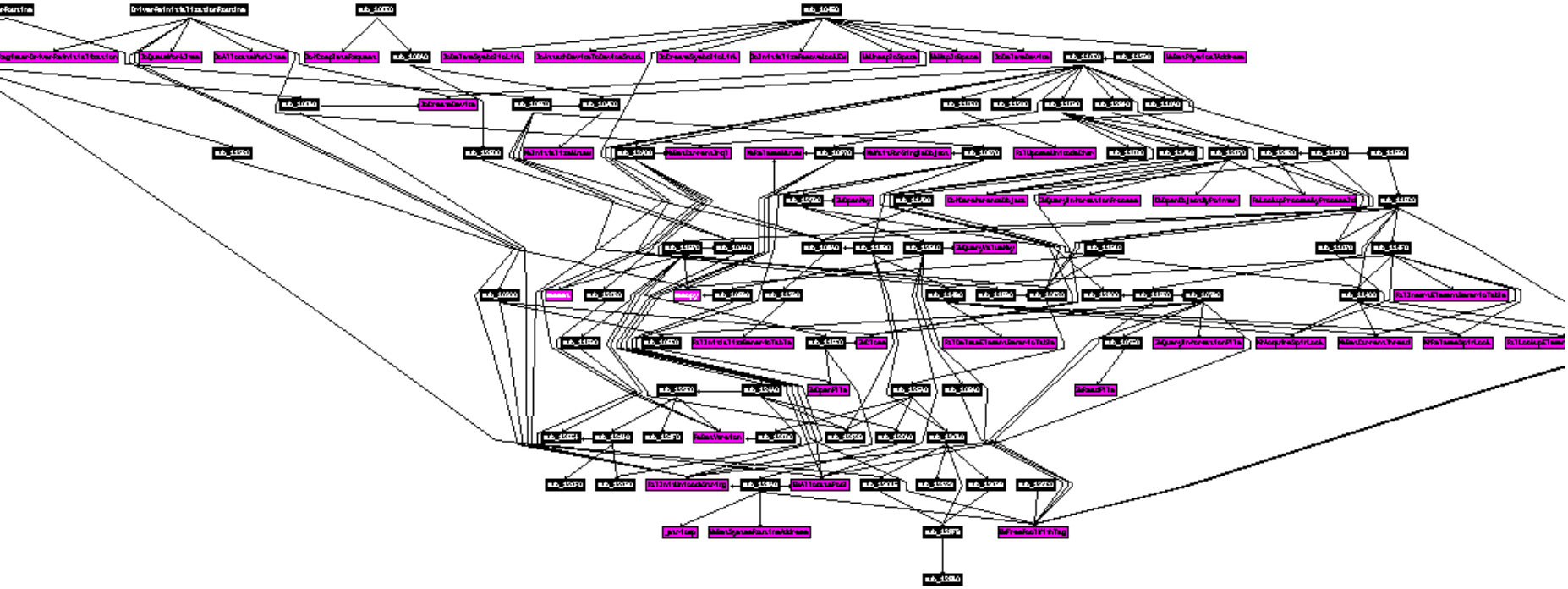
Duqu keylogger

- No detailed analysis on some functions after more than a year



Duqu kernel driver

- Still some find out interesting things in the code

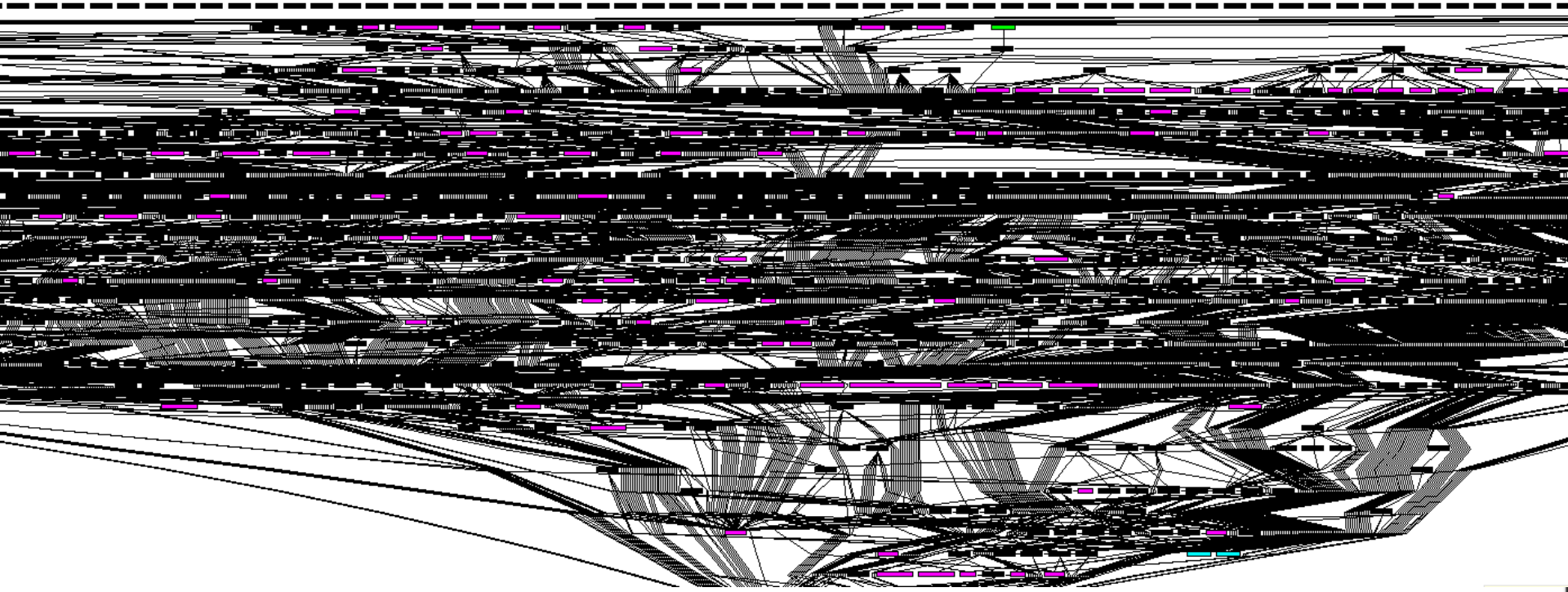


Flame Suicide Module (Browse32)

- Flame Suicide module, Browse32 is 450k large
- High complexity: Why?
- Probably static libraries

Duqu/ Netp191 main module uncompressed

- Very complex
- Maybe the main reason is statically linked libraries



Lessons learned

- current approaches to defend systems against targeted attacks are ineffective
  - code signing is not bullet proof
  - virus scanners should be extended with anomaly detection
- global threat mitigation and forensic analysis are challenging problems
  - How to share information in a privacy preserving manner?
    - crucial for identification of droppers (and potentially 0-day exploits)
  - How to capture C&C servers quickly?
  - How to track down the C&C proxy chain?
- attackers started to use advanced techniques
  - MD5 collision attack in Flame
  - encrypted payload in Gauss

What to do against similar attacks at your company?

- Extend your protection beyond signature based techniques
  - Anomaly detection
  - Heuristics
  - Baits, traps, honeypots
- Educate your team to find out anomalies
- Everybody needs forensics – you can never know what you find
- Use tools to check suspicious computer
- Check network traffic for strange patterns
- Think on information sharing policy – the community needs the help of the victims
- Create plans for imminent incident response – have professionals ready to help you

References

- **Duqu analysis**

  B. Bencsáth, G. Pék, L. Buttyán, M. Félegyházi,
  Duqu: A Stuxnet-like malware found in the wild,
  Technical Report, CrySyS Lab, BME, 14 October 2011.

  available at www.crysys.hu/targeted-attacks.html

- **Duqu paper**

  B. Bencsáth, G. Pék, L. Buttyán, M. Félegyházi,
  Duqu: Analysis, Detection, and Lessons Learned,
  ACM European Workshop on System Security (EuroSec)
  Bern, Switzerland, April 2012.

  available at www.crysys.hu/targeted-attacks.html

- **Duqu Detector Toolkit**

  www.crysys.hu/duqudetector.html

References

- **sKyWIper analysis**

  sKyWIper Analysis Team,
  sKyWIper: A complex malware for targeted attacks,
  Technical Report, CrySyS Lab, BME, 28 May 2012.

  available at www.crysys.hu/targeted-attacks.html

- **on-line Gauss Detector Service**

  gauss.crysys.hu

- **CrySyS blog site with some interesting articles on the topic including how windows update URL works**

  blog.crysys.hu

Next Steps

- There's room for innovation in defensive security technology
- We are open for collaboration

http://www.crysys.hu/

```
Duqusubmit anonymous malware submission PGP fingerprint:
E84E 7C73 C95D 65AD E7A6 A555 53C8 E4CC 17F0 A1A1
bencsath@crysys.hu PGP fingerprint
286C A586 6311 36B3 2F94 B905 AFB7 C688 64CF 6EFB
buttyan@crysys.hu PGP fingerprint
7E10 7013 706B DCD2 367C 689A 5EA5 696E 37C1 BAE1
```