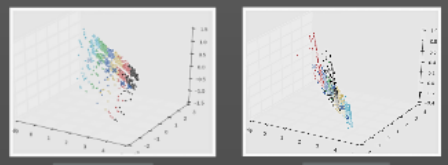
PROBLEM @ Initech

- According to a report by AppRiver, the levels of spam and malware email traffic recorded during Q1 2016 have already surpassed. This totalled 2.3 billion malicious email messages, with 1.7 billion in March.
- What is Malware?
  - * A type of malicious software cyber criminals use to infiltrate computer systems and networks
  - * Primarily with the aim to procure sensitive information or, to a lesser degree, disrupt day-to-day operations.

NO SECURITY MEASURES -->OVERHEAD -->HOTBED FOR MALWARE --> DENEID COVERAGE & FUNDING ☹

MALWARE FAMILIES

* Based on the PEinfo files used by the company in the past, 6 malicious families can be clearly visualized as compared to the benign ones.

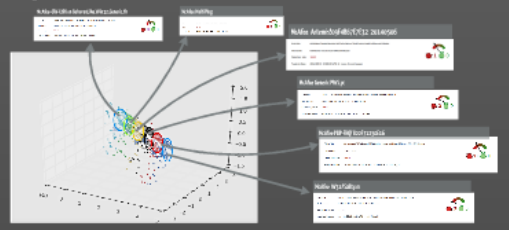


MALICIOUS EXECUTABLES

BENIGN EXECUTABLES

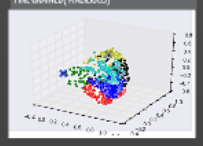
Let's Identify.....

virustotal

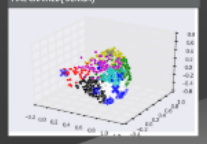


SIMILARITY (BY OBJ_DUMP)

FINE GRAINED(MALICIOUS)



FINE GRAINED(BENIGN)



SIMILARITY ALGORITHM:

1) Aanalyze Malicious and Benign Object Dump Files .

2)Analyze , PEinfo & cluster to find malware families.

3)Cluster Obj_Dump & Train the system with cluster labels.

4)Test & Predict on Peinfo (Nearest Neighbors)

5)Different Algorithms differ from original cluster(LSH,Ball Tree the best)

FEATURES ANALYZED

Concerns & Recommendations

* Similar obj_dump gives similar identification results of PEinfo.

* Silhouette Analysis provides a clear distinction of the seperation of clusters, but the inter cluster distance is less with respect to peinfo(73%) and objdump(9 1.8%)

* But Similar Peinfo result lie in different clusters of obj_dump using nearest Neighbor Algorithms.

* LSH Forest gives better results but more clusters with unevenly distributed samples.

Identify Obj_Dump Malware Executables

Feature Analysis of Categorical Data

Analyze Similarity(Every Executable with Objdump)

Use VirusTotal & Anti Malware Scanners

INITECH

THE MALWARE ENIGMA

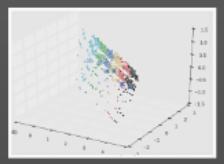
PROBLEM @ Initech

- According to a report by AppRiver, the levels of spam and malware email traffic recorded during Q1 2016 have already surpassed. This totalled 2.3 billion malicious email messages, with 1.7 billion in March.
- What is Malware?
  - * A type of malicious software cyber criminals use to infiltrate computer systems and networks
  - * Primarily with the aim to procure sensitive information or, to a lesser degree, disrupt day-to-day operations.

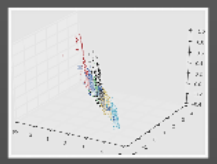
NO SECURITY MEASURES -->OVERHEAD -->HOTBED FOR MALWARE --> DENEID COVERAGE & FUNDING ☹

MALWARE FAMILIES

* Based on the PEinfo files used by the company in the past, 6 malicious families can be clearly visualized as compared to the benign ones.



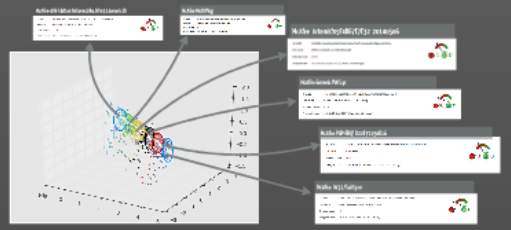
MALICIOUS EXECUTABLES



BENIGN EXECUTABLES

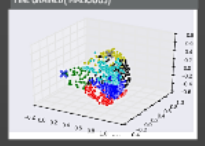
Let's Identify....

virustotal

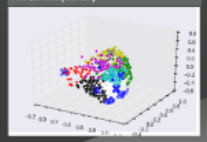


SIMILARITY (BY OBJ_DUMP)

FINE GRAINED(MALICIOUS)



FINE GRAINED(BENIGN)



SIMILARITY ALGORITHM:

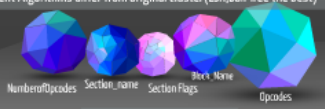
1) Aanalyze Malicious and Benign Object Dump Files .

2)Analyze , PEinfo & cluster to find malware families.

3)Cluster Obj_Dump & Train the system with cluster labels.

4)Test & Predict on Peinfo (Nearest Neighbors)

5)Different Algorithms differ from original cluster(LSH,Ball Tree the best)



FEATURES ANALYZED

Concerns & Recommendations

* Similar obj_dump gives similar identification results of PEinfo.

* Silhouette Analysis provides a clear distinction of the seperation of clusters, but the inter cluster distance is less with respect to peinfo(73%) and objdump(9 1.8%)

* But Similar Peinfo result lie in different clusters of obj_dump using nearest Neighbor Algorithms.

* LSH Forest gives better results but more clusters with unevenly distributed samples.

Identify Obj_Dump Malware Executables

Feature Analysis of Categorical Data

Analyze Similarity(Every Executable with Objdump)

Use VirusTotal & Anti Malware Scanners

INITECH

THE MALWARE ENIGMA

PROBLEM @ Initech

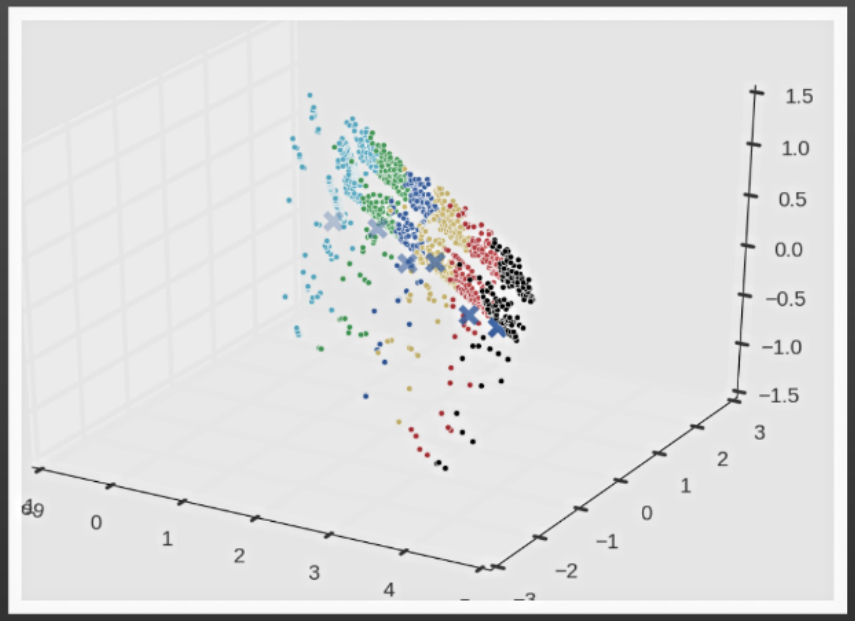
- According to a report by AppRiver, the levels of spam and malware email traffic recorded during Q1 2016 have already surpassed. This totalled 2.3 billion malicious email messages, with 1.7 billion in March.

- What is Malware?
  * A type of malicious software cyber criminals use to infiltrate computer systems and networks
  * Primarily with the aim to procure sensitive information or, to a lesser degree, disrupt day-to-day operations.

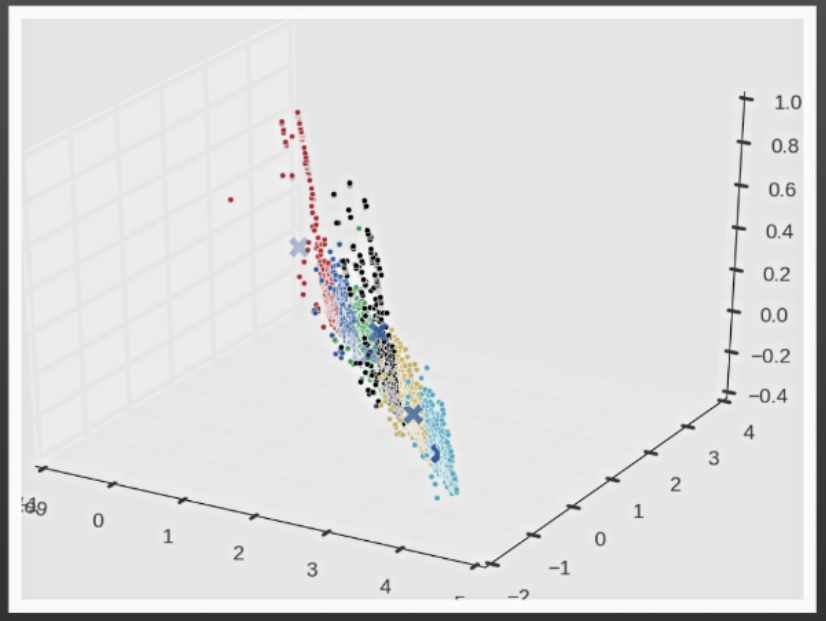
NO SECURITY MEASURES -->OVERHEAD -->HOTBED FOR MALWARE --> DENEID COVERAGE & FUNDING ☹

MALWARE FAMILIES

* Based on the PEinfo files used by the company in the past, 6 malicious families can be clearly visualized as compared to the benign ones.



MALICIOUS EXECUTABLES



BENIGN EXECUTABLES

Let's Identify.....

virustotal

McAfee-GW-Edition BehavesLike.Win32.Generic.th

McAfee MultiPlug

McAfee Artemis!09F4B67E7E32 20140506

SHA256: 00066fbfc7dcdd54bc6b43607e0e5fb1ee73b37e02da2dd53c59aeccb205dfb1
File name: 09f4b67e7e32afc42a74346af593e280
Detection rate: 16/52
Analysis Date: 2014-05-06 02:05:03 UTC (2 years, 8 months ago)

McAfee Generic PWS.yc

McAfee PUP-FHQ! 822F71250E16

SHA256: 001a48ad6757db4c4a97f83c8d6123c4a1e3b2cca2f5eafed0ffba2f6f823ca
File name: TSULoader
Detection rate: 28/51
Analysis Date: 2014-04-06 01:36:09 UTC (2 years, 9 months ago)

McAfee W32/Sality.m

Dateiname: 04d85f3048971f6415e1445fa7e40e23c.exe
Erkennungsrate: 45 / 48
Analyse-Datum: 2014-01-05 16:23:29 UTC (vor 3 Jahre)

But..What does it mean?

Generic PWS.yc

- Trojan that comes hidden in malicious programs.
- Once the program is installed, gain to attempt "root" access (administrator level access) to your computer without your knowledge.
- Hide themselves by integrating into the operating system.
- Once it infects your computer, Generic PWS.yc executes each time your computer boots and attempts to download and install other malicious files.
- Upon successful execution, it deletes the source program, making it more difficult to detect.

But..What does it mean?

PUP-FHQ! 822F71250E16

- Detected as a "potentially unwanted program" (PUP) ,not a virus or a Trojan
- This program may have legitimate uses , knowingly installed application and agreeing with license agreement may cause legal obligations with regard of renewing the software .
- PUPs are often made by a legitimate corporate entity for some beneficial purpose.
- Alter the security state of the computer on which they are installed, or the privacy posture of the user of the system, such that most users will want to be aware of them.

But..What does it mean?

W32/Sality.n

- This detection is for a Win32 parasitic virus variant that infects Windows portable executable (PE) files.
- Drops and inject the OLEMIN32.DLL file into running processes infects PE executable files
- Infected files grow in length by 20 kilobytes.
- When an infected file is run, the virus searches for other files to infect & appends configuration data into the SYSTEM.INI file
- Download additional malware from various pre-defined servers - they may be Adware SpyShetiff, BackDoor, Proxy, KeyLogger or other PUPs and trojans.

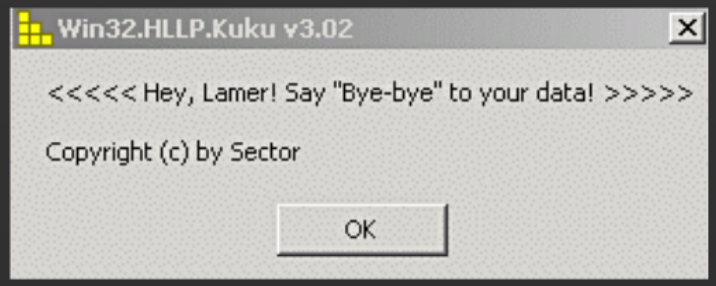
Concerns..Are there any?

- Infect executable files on local, removable and remote shared drives by replacing the original host code at the entry point of the executable to redirect execution to the polymorphic viral code, which has been encrypted and inserted in the last section of the host file.
- Purposely search for specific registry sub-keys to infect the executable files that run when Windows starts.
- A sneaky computer threat that hides itself in the registry files of a compromised computer , modifies a computer's settings thereby making it vulnerable to attackers and giving them access to a victim's sensitive information.
- Ruins Web browsing experience by inserting ads throughout Web pages you visit, redirecting search engine queries and displaying pop-up advertisements

But..What does it mean?

W32/Sality.m

* This detection is for a Win32 parasitic virus variant that infects Windows portable executable (PE) files.
* Drops and inject the OLEMDB32.DLL file into running processes infects PE executable files
* Infected files grow in length by 20 kilobytes.
* When an infected file is run, the virus searches for other files to infect & appends configuration data into the SYSTEM.INI file
* Download additional malware from various pre-defined servers - they may be Adware-SpySheriff , BackDoor, Proxy, KeyLogger or other PUPs and trojans.



But..What does it mean?

Generic PWS.yc

* Trojan that comes hidden in malicious programs.

* Once the program is installed, gain to attempt "root" access (administrator level access) to your computer without your knowledge.

* Hide themselves by integrating into the operating system.

* Once it infects your computer, Generic PWS.yc executes each time your computer boots and attempts to download and install other malicious files.

* Upon successful execution, it deletes the source program, making it more difficult to detect.

But..What does it mean?

PUP-FHQ! 822F71250E16

* Detected as a "potentially unwanted program" (PUP) ,not a virus or a Trojan

* This program may have legitimate uses , knowingly installed application and agreeing with license agreement may cause legal obligations with regard of removing the software .

* PUPs are often made by a legitimate corporate entity for some beneficial purpose.

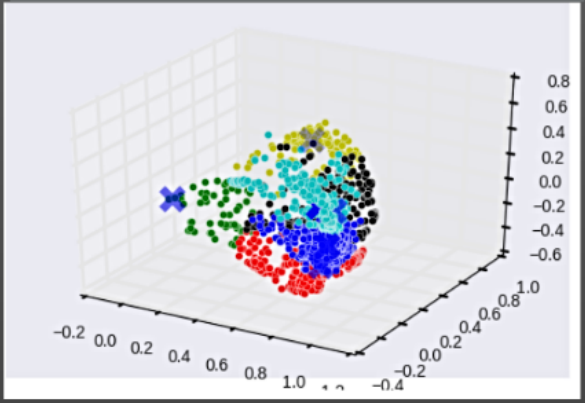
* Alter the security state of the computer on which they are installed, or the privacy posture of the user of the system, such that most users will want to be aware of them.

Concerns..Are there any?

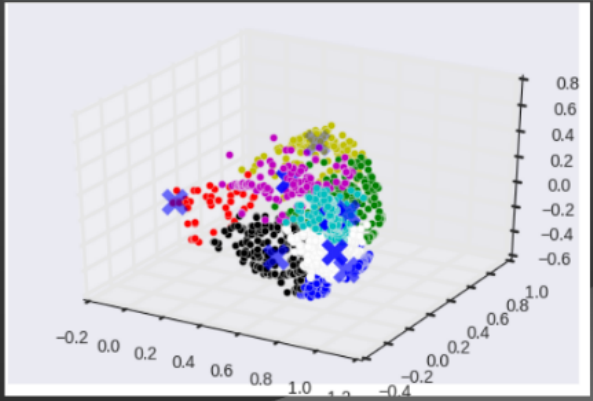
- Infect executable files on local, removable and remote shared drives by replacing the original host code at the entry point of the executable to redirect execution to the polymorphic viral code, which has been encrypted and inserted in the last section of the host file.
- Purposely search for specific registry sub-keys to infect the executable files that run when Windows starts.
- A sneaky computer threat that hides itself in the registry files of a compromised computer , modifies a computer's settings thereby making it vulnerable to attackers and giving them access to a victim's sensitive information.
- Ruins Web browsing experience by inserting ads throughout Web pages you visit, redirecting search engine queries and displaying pop-up advertisements

SIMILARITY (BY OBJ_DUMP)

FINE GRAINED(MALICIOUS)



FINE GRAINED(BENIGN)



SIMILARITY ALGORITHM:

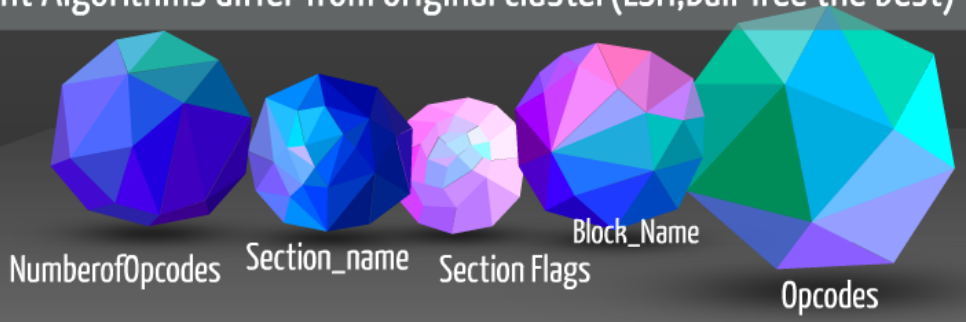
1) Aanalyze Malicious and Benign Object Dump Files .

2)Analyze , PEinfo & cluster to find malware families.

3)Cluster Obj_Dump & Train the system with cluster labels.

4)Test & Predict on Peinfo (Nearest Neighbors)

5)Different Algorithms differ from original cluster(LSH,Ball Tree the best)



FEATURES ANALYZED

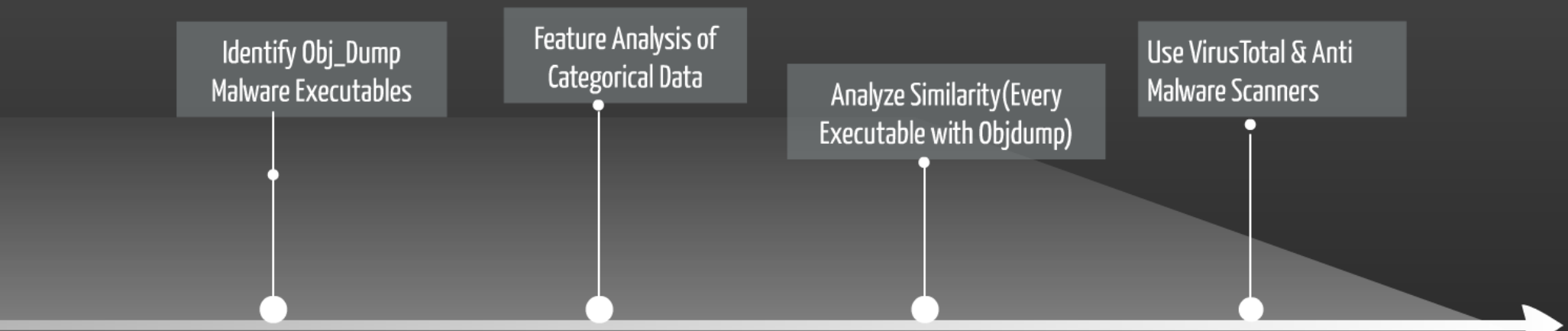
Concerns & Recommendations

* Similar obj_dump gives similar identification results of PEinfo.

* Silhouette Analysis provides a clear distinction of the seperation of clusters, but the inter cluster distance is less with respect to peinfo(73%) and objdump(9 1.8%)

* But Similar Peinfo result lie in different clusters of obj_dump using nearest Neighbor Algorithms.

* LSH Forest gives better results but more clusters with unevenly distributed samples.



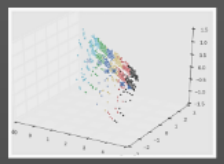
PROBLEM @ Initech

- According to a report by AppRiver, the levels of spam and malware email traffic recorded during Q1 2016 have already surpassed. This totalled 2.3 billion malicious email messages, with 1.7 billion in March.
- What is Malware?
  - * A type of malicious software cyber criminals use to infiltrate computer systems and networks
  - * Primarily with the aim to procure sensitive information or, to a lesser degree, disrupt day-to-day operations.

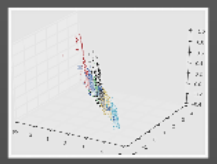
NO SECURITY MEASURES -->OVERHEAD -->HOTBED FOR MALWARE --> DENEID COVERAGE & FUNDING ☹

MALWARE FAMILIES

* Based on the PEinfo files used by the company in the past, 6 malicious families can be clearly visualized as compared to the benign ones.



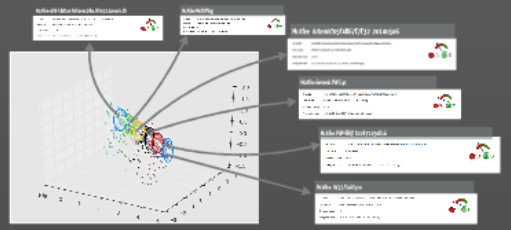
MALICIOUS EXECUTABLES



BENIGN EXECUTABLES

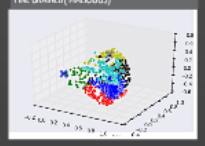
Let's Identify....

virustotal

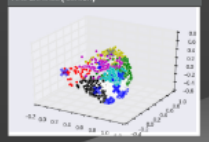


SIMILARITY (BY OBJ_DUMP)

FINE GRAINED(MALICIOUS)



FINE GRAINED(BENIGN)



SIMILARITY ALGORITHM:

1) Aanalyze Malicious and Benign Object Dump Files .

2)Analyze , PEinfo & cluster to find malware families.

3)Cluster Obj_Dump & Train the system with cluster labels.

4)Test & Predict on Peinfo (Nearest Neighbors)

5)Different Algorithms differ from original cluster(LSH,Ball Tree the best)

FEATURES ANALYZED

Concerns & Recommendations

* Similar obj_dump gives similar identification results of PEinfo.

* Silhouette Analysis provides a clear distinction of the seperation of clusters, but the inter cluster distance is less with respect to peinfo(73%) and objdump(9 1.8%)

* But Similar Peinfo result lie in different clusters of obj_dump using nearest Neighbor Algorithms.

* LSH Forest gives better results but more clusters with unevenly distributed samples.

Identify Obj_Dump Malware Executables

Feature Analysis of Categorical Data

Analyze Similarity(Every Executable with Objdump)

Use VirusTotal & Anti Malware Scanners

INITECH

THE MALWARE ENIGMA