The Importance of Security Intelligence in Protecting Customer Data and Corporate Assets

By: Ramses Martinez

Director Malicious Code Operations

iDefense, a VeriSign Company

Where it all comes together.

Agenda

- **Goal**
- **Defining the Problem**
- **Solutions**
- **Intelligence in Action (Case Studies)**

Goal

To provide and Enterprise with timely information on cyber related threats which result in better management of risk.

Defining the Problem

Complexity of the Threat

+ Targeted attacks
+ Zero-day vulnerabilities
+ Exploitation with criminal intent
+ Fast spreading worms

Defining the Problem (Cont.)

Sources

+ Dozens of security mailing lists
+ Hundreds of security websites
+ Hundreds of information security news outlets

Defining the Problem (Cont.)

Reporting

+ Conflicting or incorrect information
+ Amplification effect
+ Repeating inaccurate information
+ Inaccurate threat assessment
+ No actionable data

Defining the Problem (Cont.)

Timing

+ News, not intelligence
+ Too late to be actionable
+ No trend and forecasting component

Solution

Bringing it All Together

+ Aggregate data from public sources
+ Process/Filter data
+ Augment with data from private sources
+ Expert verification
+ Threat Assessment

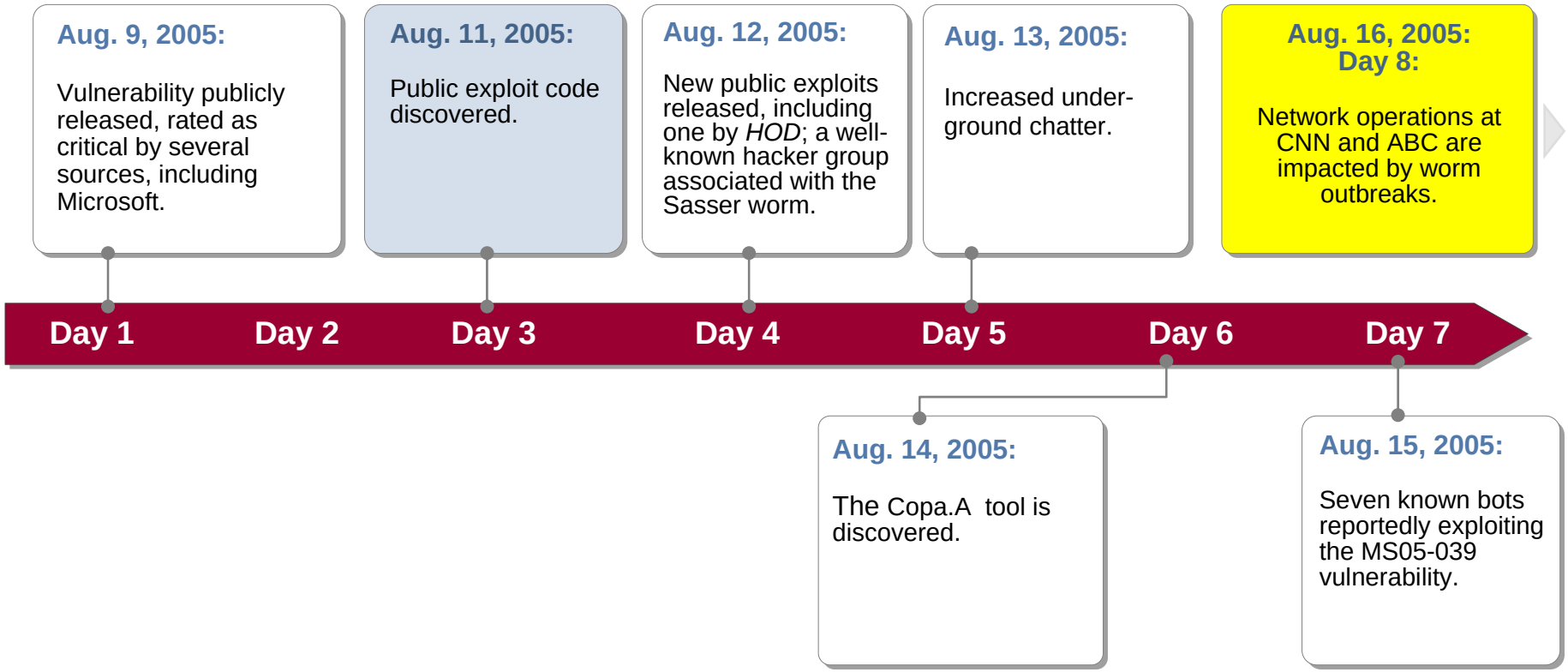
The Difference Between MS-039 and MS-051

+ When to Emergency Patch
  - ZoTob/MS05-039
+ When ***Not*** to Emergency Patch
  - MS-051/Large Financial Company example
  - $1.5M Saved

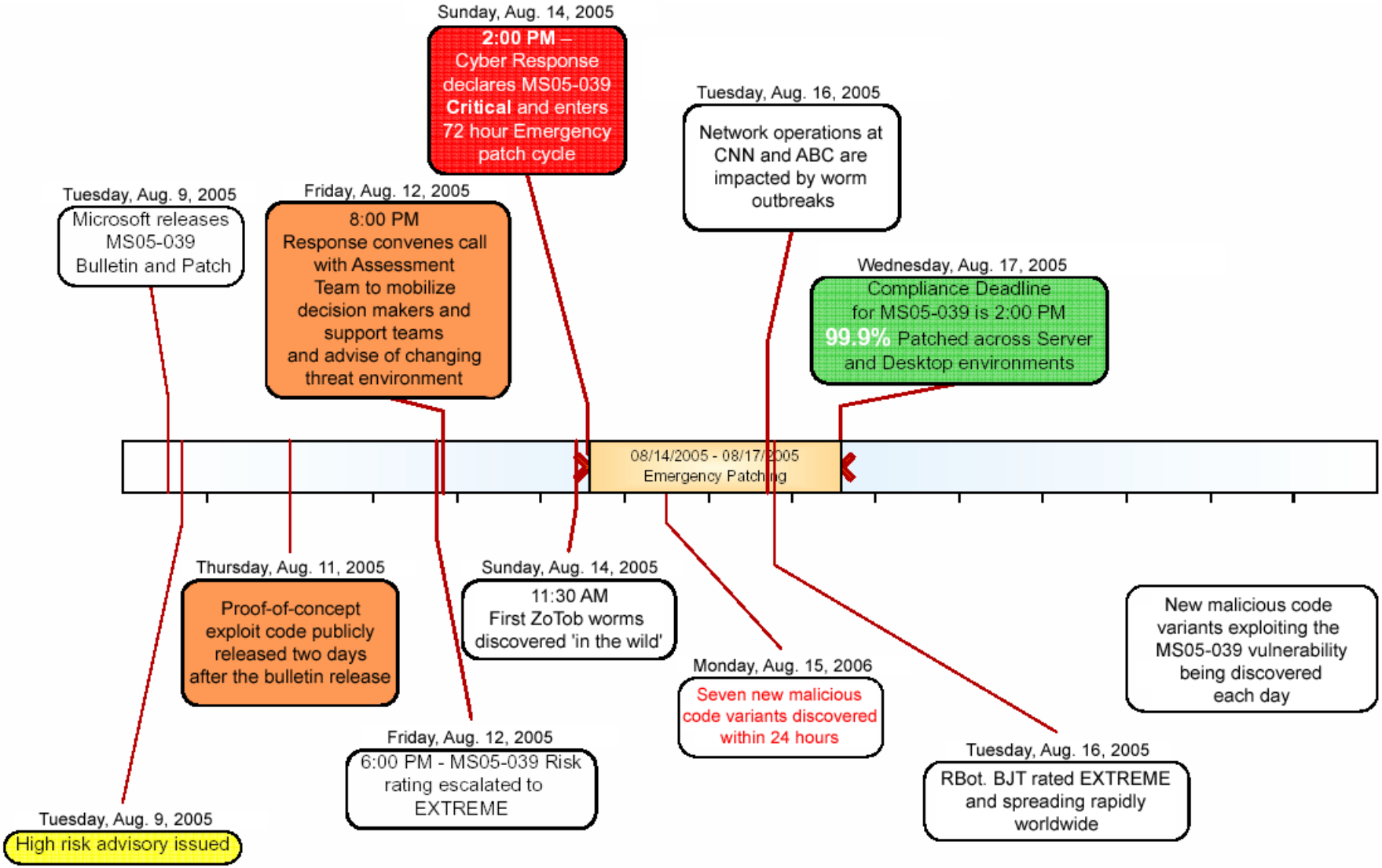
Why is PnP/ZoTob Important?

+ Attack speed
+ Actors involved are important, and the threat is critical
+ Underground activity
+ Intelligence gathering and analysis is key

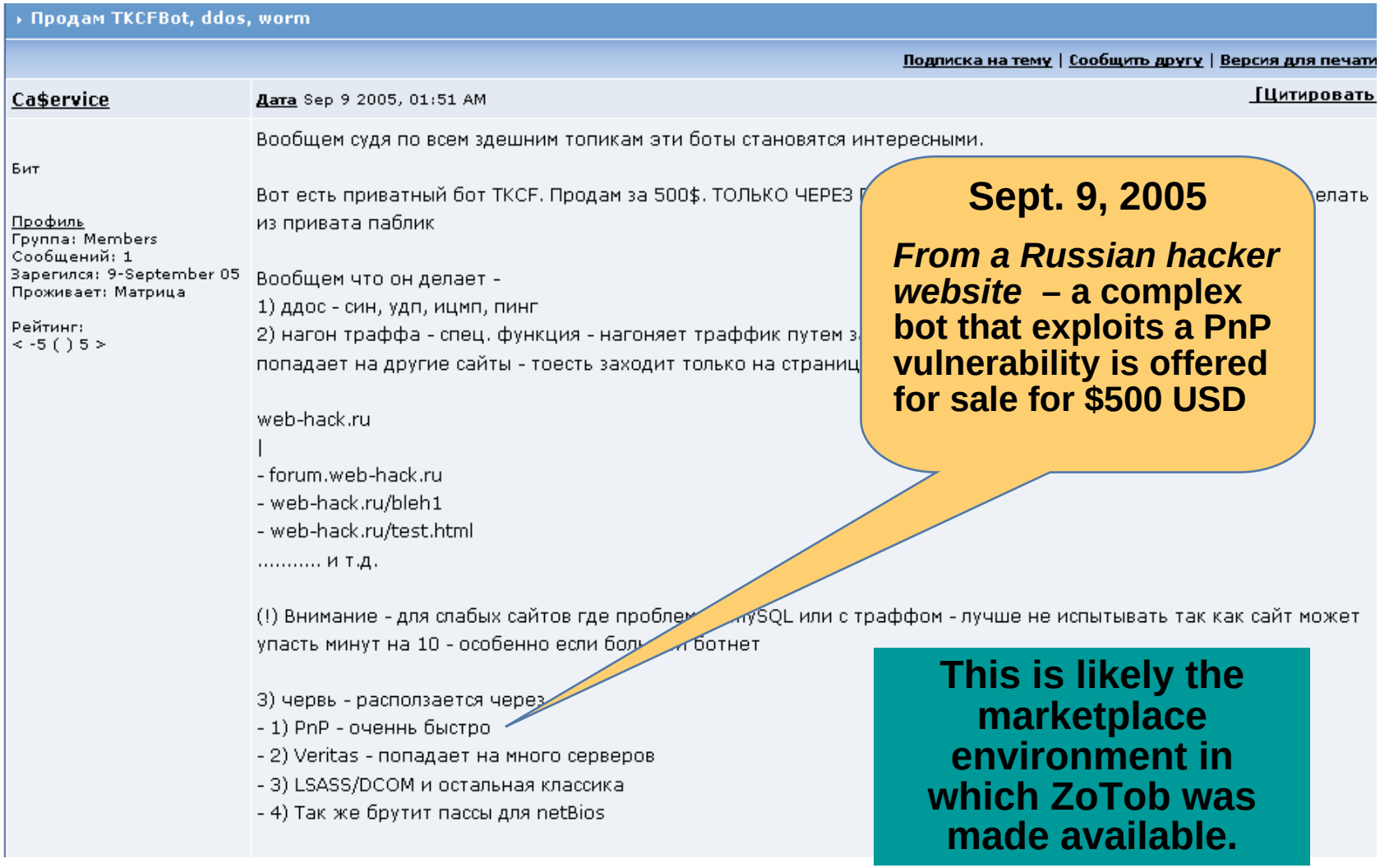
MS05-039 PnP (ZoTob.A) Case Study



Financial Customer's Timeline



“Diabl0” and “C0der”



▸ Продам TKCFBot, ddos, worm

Подписка на тему | Сообщить другу | Версия для печати

Ca$ervice — **Дата** Sep 9 2005, 01:51 AM — [Цитировать

Бит

Профиль
Группа: Members
Сообщений: 1
Зарегился: 9-September 05
Проживает: Матрица

Рейтинг:
< -5 ( ) 5 >

Вообщем судя по всем здешним топикам эти боты становятся интересными.

Вот есть приватный бот TKCF. Продам за 500$. ТОЛЬКО ЧЕРЕЗ … елать из привата паблик

Вообщем что он делает -
1) ддос - син, удп, ицмп, пинг
2) нагон траффа - спец. функция - нагоняет траффик путем з…
попадает на другие сайты - тоесть заходит только на страниц…

web-hack.ru
|
- forum.web-hack.ru
- web-hack.ru/bleh1
- web-hack.ru/test.html
..... и т.д.

(!) Внимание - для слабых сайтов где проблем… mySQL или с траффом - лучше не испытывать так как сайт может упасть минут на 10 - особенно если боль… ботнет

3) червь - расползается через
- 1) PnP - оченнь быстро
- 2) Veritas - попадает на много серверов
- 3) LSASS/DCOM и остальная классика
- 4) Так же брутит пассы для netBios

Sept. 9, 2005

From a Russian hacker website **– a complex bot that exploits a PnP vulnerability is offered for sale for $500 USD**

This is likely the marketplace environment in which ZoTob was made available.

MS05-051 – When ***Not*** to Implement Emergency Procedures

- Three vulnerabilities in MS05-051 are discovered in March
- The release of MS05-051 generated very little underground activity, as compared to MS05-039 in August.
- Privately traded exploit code exists, but is not in the hands of known actors or in the wild.
- It is confirmed that this vulnerability could be exploited over TCP port 1025.
- Simply blocking TCP port 3372 (the port on which MSDTC listens) did ***not*** eliminate the threat posed by this issue.
- Functional malicious code has not been seen in the wild.

Q/A

By: Ramses Martinez

Director Malicious Code Operations

iDefense, a VeriSign Company

Where it all comes together.