Know when to Patch – Save money from unnecessary patching

Introduced by Nadine Dereza

Mike Davies

EMEA Marketing Director

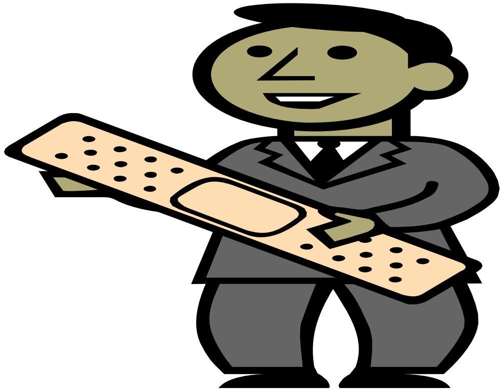
Where it all comes together.

Patching

- The IT environment is becoming even more complex

- Increasing threats from vulnerabilities and malicious sources

- Cost of patching can run into millions annually and take up valuable resource

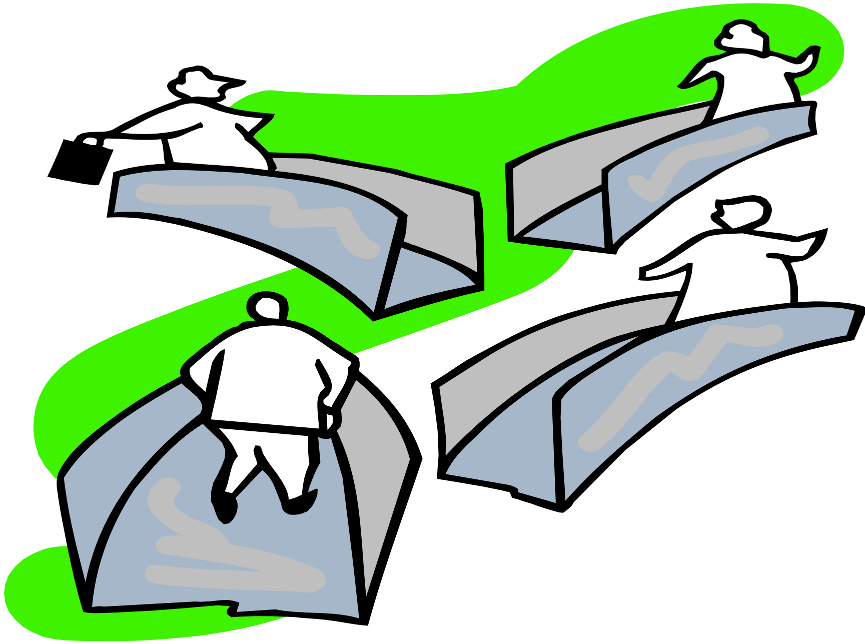


How do we prevent unnecessary patching?

By providing an Enterprise with timely information on cyber related threats which result in better management of risk

The problem – Complexity of the threat

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

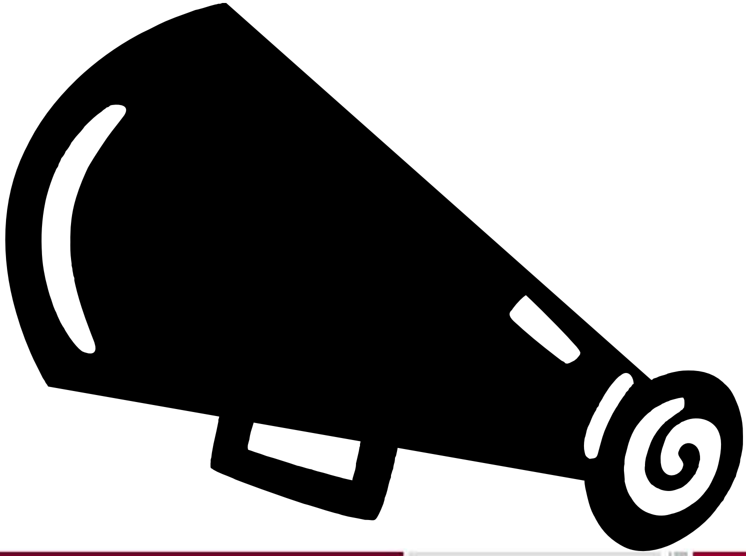


The problem – Multiple sources

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

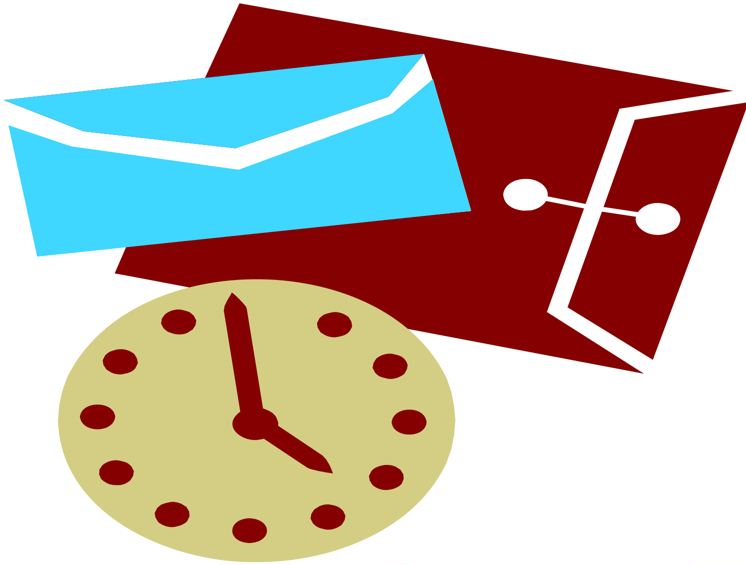
The problem - Reporting

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



The problem - Timing

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



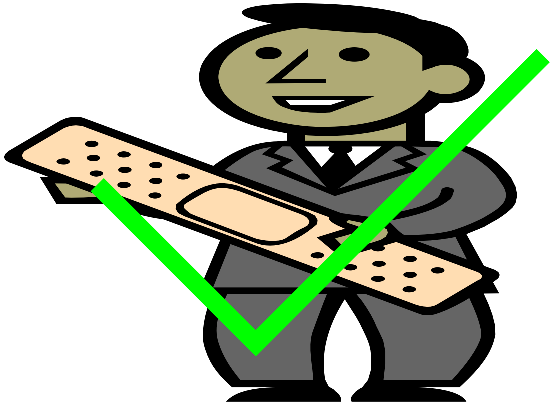
The solution – Bringing it all together

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

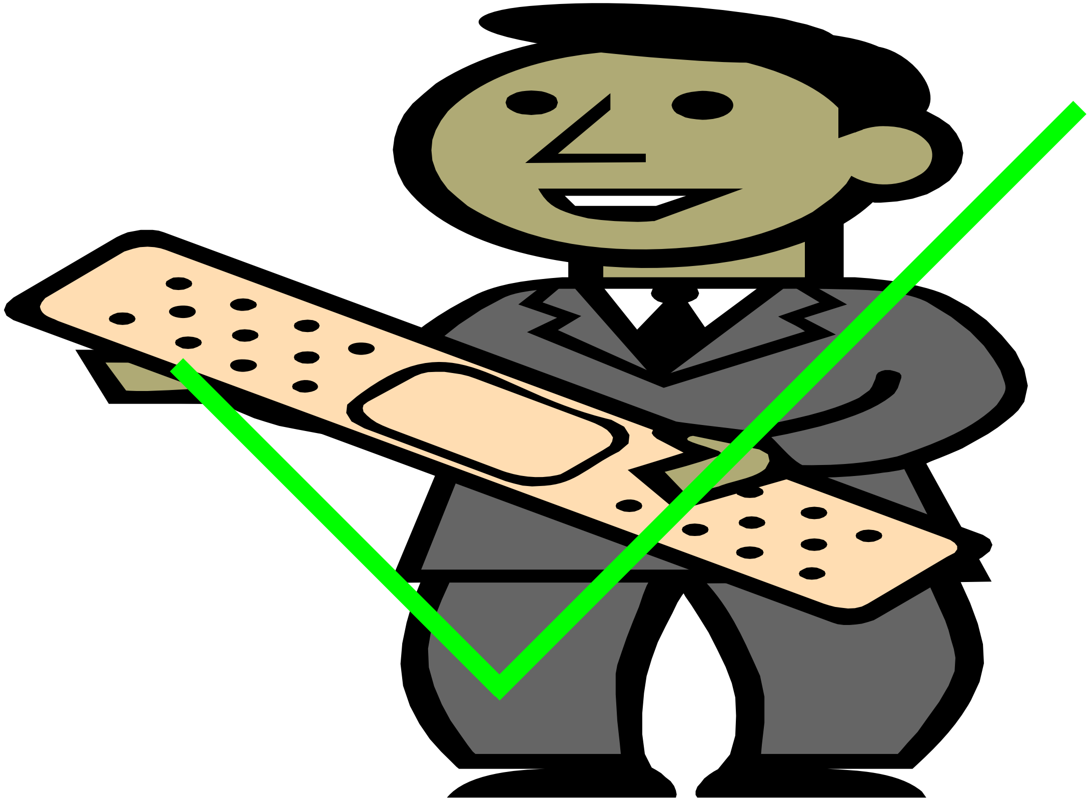
The Difference Between MS05-039 and MS05-051

+ When to Emergency Patch
  - MS05-039

+ When ***Not*** to Emergency Patch
  - MS05-051
  - Large financial customer saved $1.5M

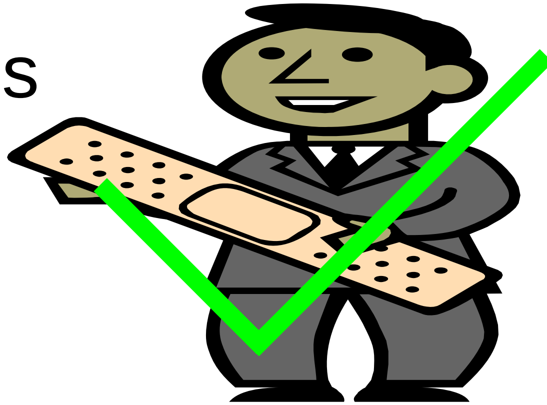


When to Patch – MS05-39

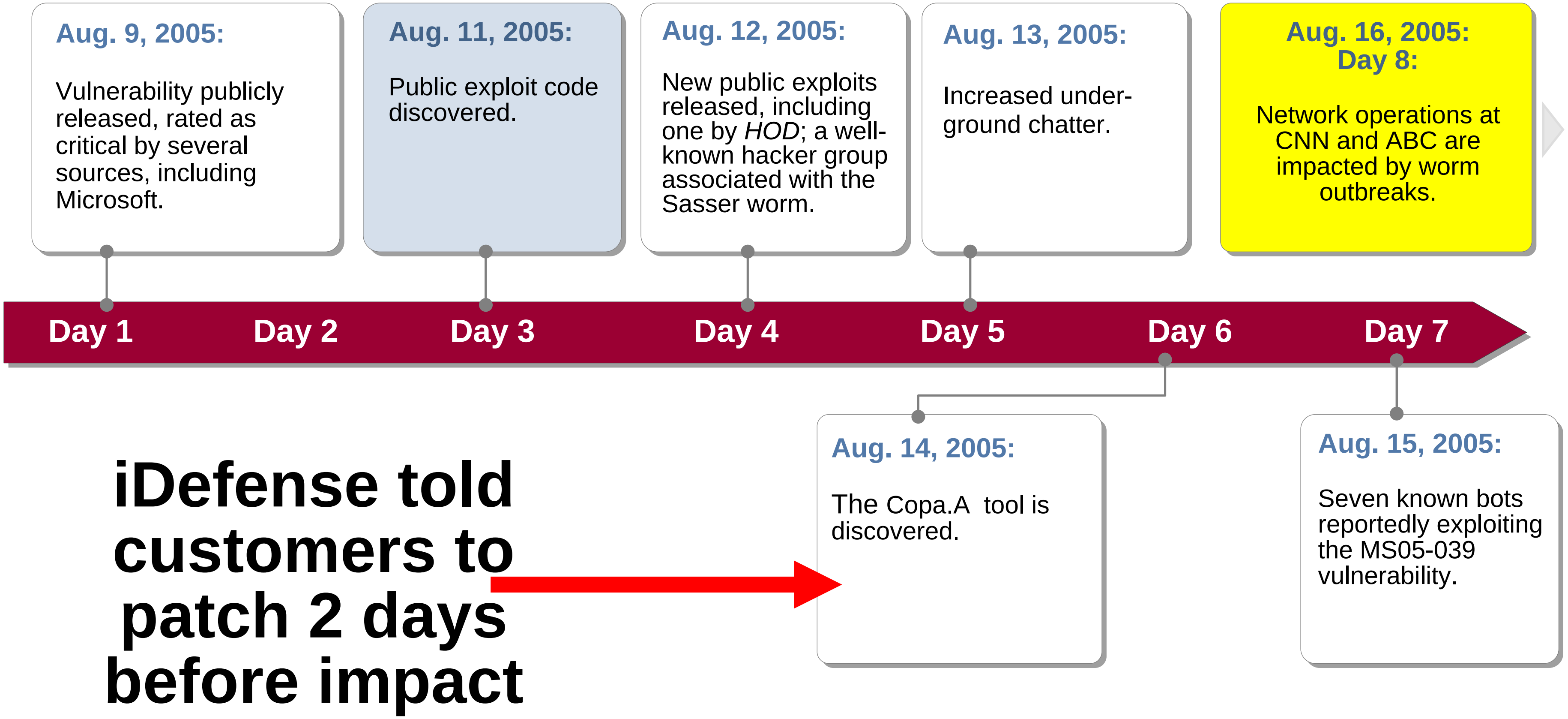


When to Patch – MS05-39, why?

- PnP was exploited by ZoTob
- Attack speed
- Actors involved important, and threat is critical
- Underground activity
- Intelligence gathering and analysis is key



MS05-039 PnP (ZoTob.A) Case Study



Aug. 9, 2005:

Vulnerability publicly released, rated as critical by several sources, including Microsoft.

Aug. 11, 2005:

Public exploit code discovered.

Aug. 12, 2005:

New public exploits released, including one by *HOD*; a well-known hacker group associated with the Sasser worm.

Aug. 13, 2005:

Increased under-ground chatter.

Aug. 16, 2005: Day 8:

Network operations at CNN and ABC are impacted by worm outbreaks.

Aug. 14, 2005:

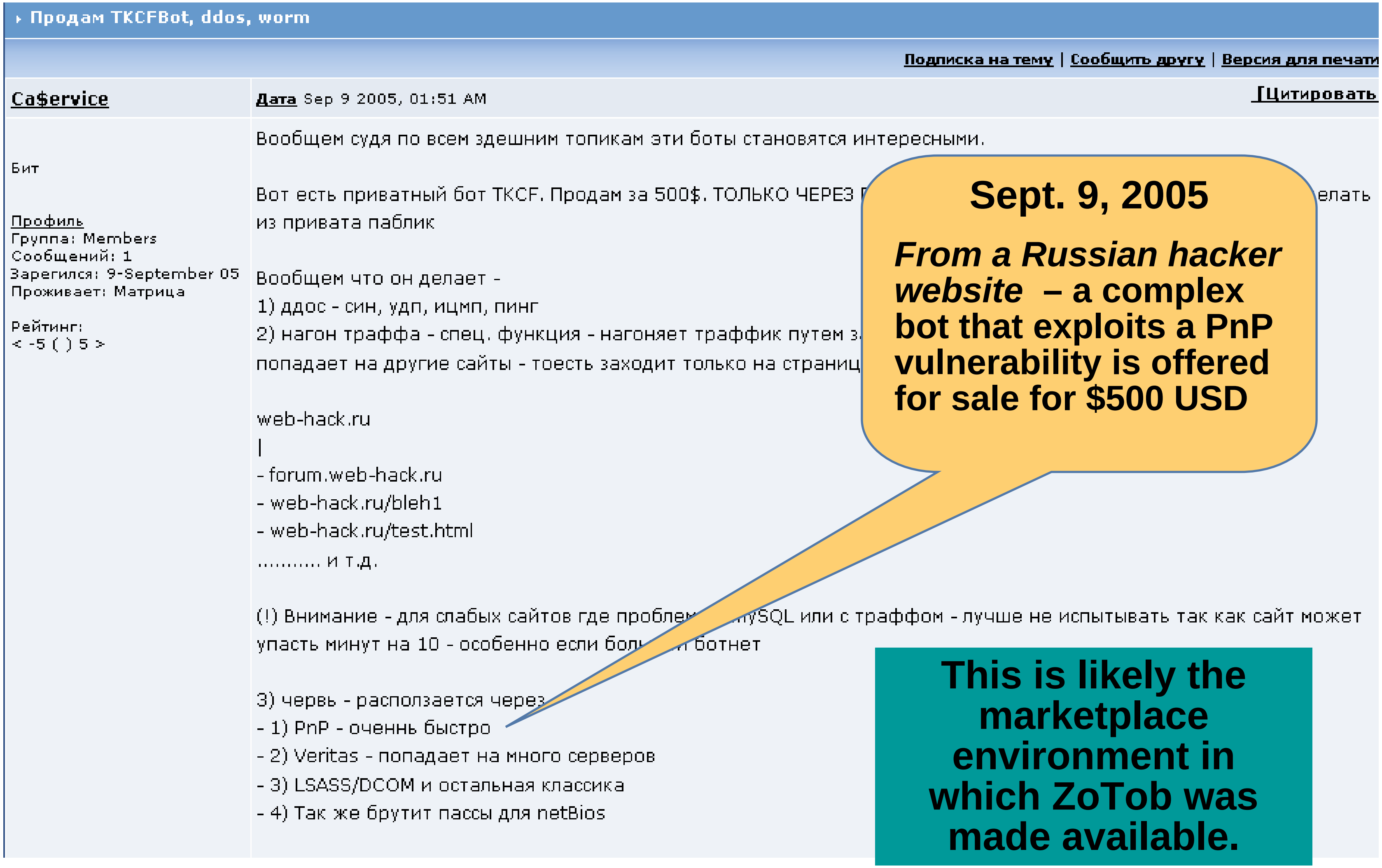
The Copa.A tool is discovered.

Aug. 15, 2005:

Seven known bots reportedly exploiting the MS05-039 vulnerability.

iDefense told customers to patch 2 days before impact

“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 Г 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 пробле ySQL или с траффом - лучше не испытывать так как сайт может
упасть минут на 10 - особенно если бол ботнет

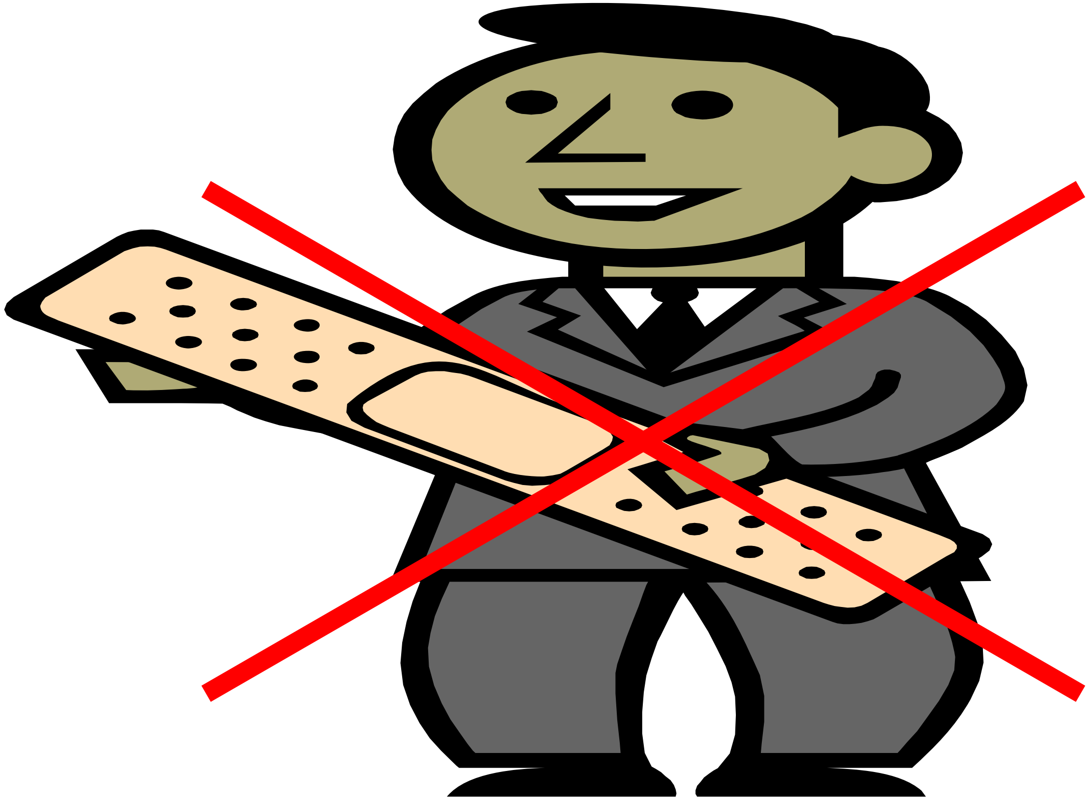
3) червь - расползается через
- 1) PnP - оченнь быстро
- 2) Veritas - попадает на много серверов
- 3) LSASS/DCOM и остальная классика
- 4) Так же брутит пассы для netBios

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.

When NOT to Patch – MS05-39

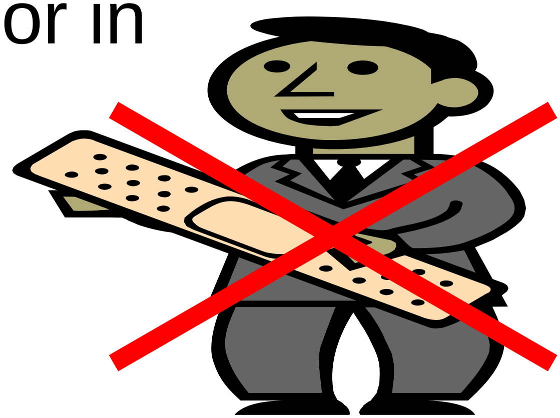


MS05-051 – When ***Not*** to Implement Emergency Procedures

- 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



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

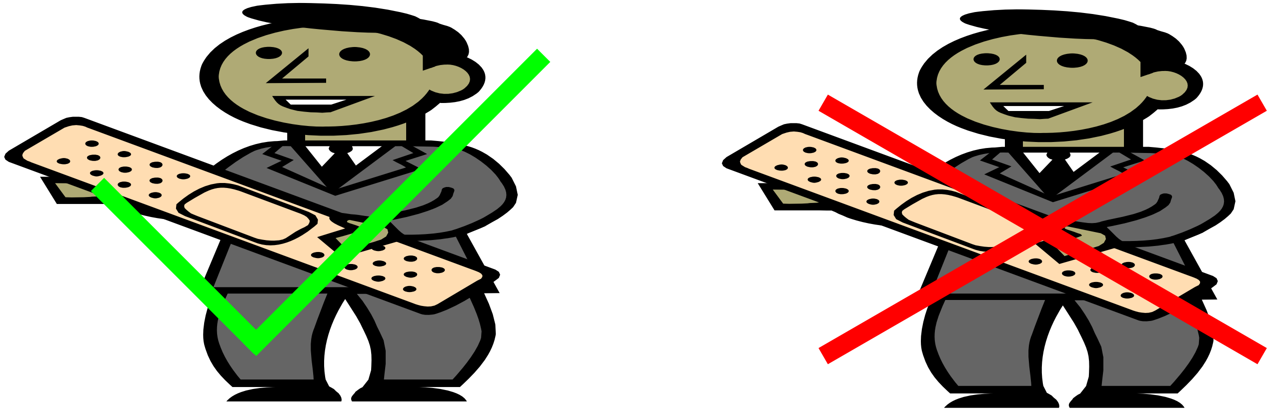
- It is confirmed that this vulnerability could be exploited over TCP port 1025.
- Simply blocking TCP port 3372 (the port on which MSDTC listens) did ***not*** eliminate the threat posed by this issue.
- Functional malicious code has not been seen in the wild

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

- Other sources instructed people to emergency patch
- Example of amplication effect of unverified information
- iDefense customers told not to patch
- Large Financial customer saved $1.5m by not breaking normal patching cycle

In summary

Deep threat intelligence provided by iDefense can help you make the right decision on patching saving you time and money



Know when to Patch – Save money from unnecessary patching

Introduced by Nadine Dereza

Mike Davies

EMEA Marketing Director

Where it all comes together.