TURLA LIGHTNEURON

One email away from remote code execution

Mario Leonardo Salinas

UniPi - ICT Risk Assessment

- 1. Introduction
- 2. Attacker Profile & Victimology
- 3. Tools & Tactics
- 4. Impact
- 5. Countermeasures
- 6. Conclusions

Introduction

Attacker Profile & Victimology

Tools & Tactics

Impact

Countermeasures

Turla

- Turla, aka *Snake*, is one of the oldes and still active cyberespionage gruops [1]
- High profile targets:
 - USA Dept. of Defence Swiss defense company RUAG European goverments
- The group owns a large arsenal of malware and backdoors

LightNeuron

- LightNeuron is a *malware* specifically designed to target Micrsoft Exchange servers.
- It can spy on emails and act as a fully featured backdoor
- Hard to detect at the network level (no standard HTTP(s) communications)

Introduction

Attacker Profile & Victimology

Tools & Tactics

Impact

Countermeasures

Metropolis

The **metropolis** theme is a Beamer theme with minimal visual [3] noise inspired[4] by the HSRM Beamer Theme by Benjamin Weiss.

Enable the theme by loading [2]

```
\documentclass{beamer}
\usetheme{metropolis}
```

Note, that you have to have Mozilla's *Fira Sans* font and XeTeX installed to enjoy[5] this wonderful typography.

Introduction

Attacker Profile & Victimology

Tools & Tactics

Impact

Countermeasures

Tools & Tactics

- 1. the malware
- 2. the backdoor

The Malware

Light neuron is a rootkit

Introduction

Attacker Profile & Victimology

Tools & Tactics

Impact

Countermeasures

Impact

very high

Introduction

Attacker Profile & Victimology

Tools & Tactics

Impact

Countermeasures

Countermeasures

some IoCs are...

Introduction

Attacker Profile & Victimology

Tools & Tactics

Impact

Countermeasures

Conclusions

very dangerous rootkit with specific and high profile targets

References i

- [1] Matthieu Faou. Eset research white paper: Turla lightneuron, one email away from remote code execution. Technical report.
- [2] R.L. Graham, D.E. Knuth, and O. Patashnik. Concrete mathematics. Addison-Wesley, Reading, MA, 1989.
- [3] D.E. Knuth. Two notes on notation. *Amer. Math. Monthly*, 99: 403–422, 1992.
- [4] D.E. Knuth Rfa Rwegrgea and O. Patashnik. *Concrete mathematicos*. Addison-Weslo, Carosino, MA, 1989.
- [5] Homero Junior Simpson. Proof of the Riemann Hypothesis. preprint (2003), available at http://www.math.drofnats.edu/riemann.ps, 2003.