

Bad Romance: Three Reasons Hackers <3 Your Web Apps & How to Break Them Up

SESSION ID: SP01-R02



JD Sherry

Vice President, Technology & Solutions
@jdsherry



Discussion Outcomes

1. What Do They Want?
2. How Did We Get Here?
3. Weapons Grade Arsenal
4. Low Hanging Fruit-Web Apps!
5. Cost Effective Counter Measures



How Did We Get Here? Some Simple Google Fu!

- Google Dorking/Hacking Trending UP...
- Easily Boil the Ocean!
- Vulnerabilities Found in Milliseconds
- Find the needle in the haystack of needles

SHODAN EXPLOITS target.com type:webapps Search

Q:Results found: 127

Platform

php	114
asp	7
multiple	2
linux	2
cgi	1

Author

the_day	11
K-159	7
AlphaNIX	5
cjfer	4
Matthule	4

BCWb <= 0.99 (root_path) Remote File Include Vulnerability by aljann

webapps

```
#!/target.com/command.php?
\nexample:
http://target.com/include/startup.inc.php?root_path=http://target.com/
# aljann,turkey
# ...
# In not Hacker!
# mlwrm.com (2006-09-19)
```

Joomla Component com_pinboard Remote File Upload Vulnerability by VilkuMaN

webapps

```
#####
Dork inurl:com_pinboard
Exploste :
1-target.com[path]/components/com_pinboard/popup.php?option=showload
or
```

GOOGLE HACKING-DATABASE

Welcome to the google hacking database

We call them 'googledorks': Inept or foolish people as revealed by Google. Whatever you call these fools, you've found the center of the Google Hacking Universe!

Search Google Dorks

Category: All Free text search: Search

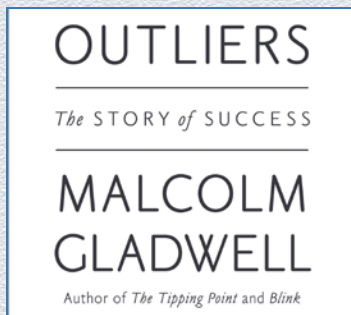
Latest Google Hacking Entries

Date	Title	Category
2014-01-03	allinurl:"/main/auth/profile.php"-github...	Pages containing login portals
2014-01-03	intitle:"=[1n73ct10n privat shell]="	Footholds
2014-01-03	intitle:"WSO 2.4" [Sec. Info], [Files...	Footholds
2013-12-03	inurl:/administrator/index.php?autologin=1	Pages containing login portals
2013-11-27	inurl:mikrotik filetype:backup	Files containing juicy info
2013-11-27	intext:phpMyAdmin SQL Dump filetype:sql intext:INS...	Files containing juicy info
2013-11-25	site:github.com inurl:sftp-config.json intext:/wp...	Files containing passwords
2013-11-25	site:github.com inurl:sftp-config.json	Files containing passwords
2013-11-25	inurl:github.com intext:sftp-conf.json +intext:/wp...	Files containing juicy info
2013-11-25	allinurl:"owa/auth/logon.aspx"-google ...	Pages containing login portals



What Do They Want? It's All About the Benjamins...

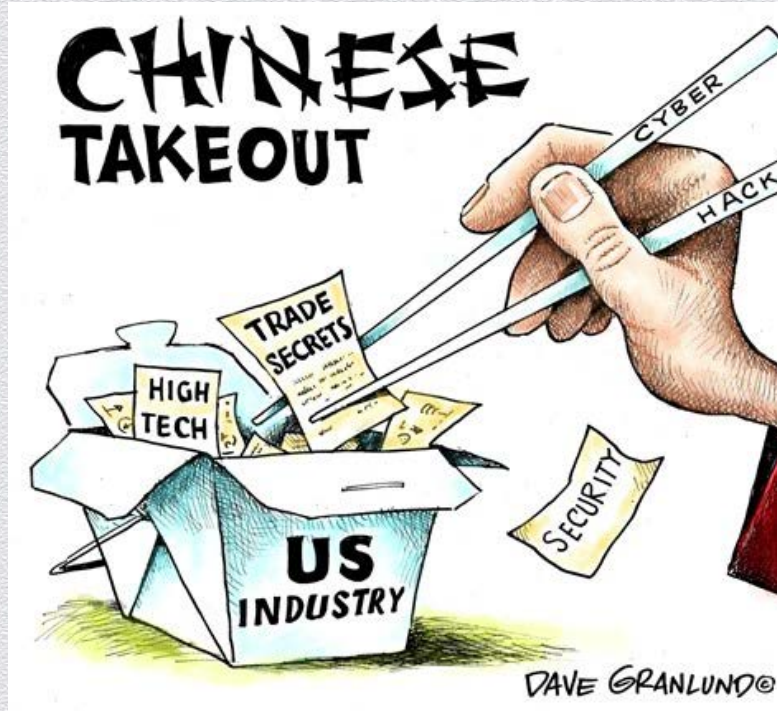
- **75%¹ Attacks focused on economic gain**
 - **94.5% of World Currency is Electronic**
- **20%¹ Attacks are state sponsored/secrets**
- **Professionalism and Business Model Proliferation²**
 - Consulting Services (\$350+)
 - Infection/Spreading Services (\$100 per 1k installs)
 - Botnet Rentals (\$2- \$600+)
 - VPN (\$7+)
 - Bulletproof Hosting (\$3/month)
 - AV Crypters (\$10/month)
 - Mule/Casher Services (25%-30% commission)



Report 2013

2-Source: Kyle Wilhoit- Sr. Threat Researcher-Trend Micro

Yes, the Chinese are still very relevant but...



Weapons Grade Arsenal

- **We are facing a “weapons grade threat”**. *Sam Visner, VP and General Manager-CSC Global Cybersecurity*
- **Eastern Euros Executing on a High Level**
 - Russian organized crime fully migrating to Cyber in 2014
 - Top Collaboration Forums
 - antichat.ru
 - xeka.ru
 - carding-cc.com
 - hackforums.net
- **Key Tactics Leveraged:**
 - Spear phishing attacks
 - Lateral movement
 - Targeting weakest link in the chain (Often Humans)
 - Persistency
 - Data theft




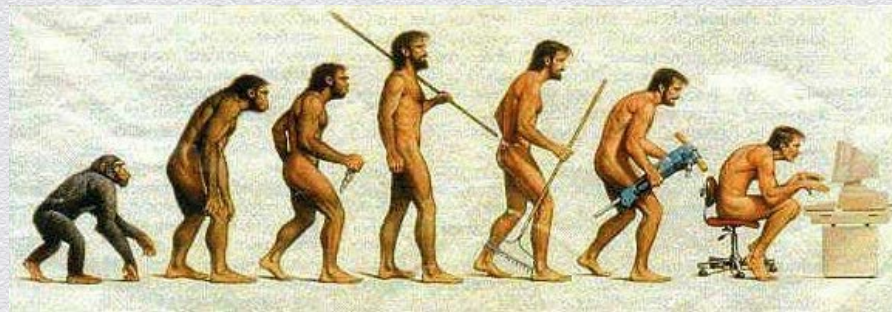
Weapons Grade Arsenal

Goals and Desired Outcomes

- Build on available technology - can't wait for new breakthroughs (no magic)
- Undetectable by anti-virus
- Stealth - undetectable by forensics investigation
- Able to withstand normal disinfection methods like reinstalling OS
- Calling home should be undetected by data leak prevention and IPS/IDS
- Able to penetrate the most secure computers even those with air gap (no connection to the internet)
- Data extraction, command and control even across an air gap

Cyber Arms Bazaar

- Seeing tool utilization “bleed over”
 - Citadel (Arx Group)
 - Zeus
 - Miniduke
 - Z-Lom
 - Utilization of 0-days
 - Had access to CVE 2013-3906 before researchers identified. (Sept. 2013)
- 
- An illustration showing the progression of human evolution from an ape-like ancestor on the left to a modern human on the right. The figures are shown in a line, with the first being a crouching ape, followed by two intermediate hominids, and finally a modern human standing upright and holding a tool.



Web App Security Challenges

Proliferation of web apps
High value target



Many different applications and security solutions



Hard to get single view

Frequent app changes
Infrequent testing



Scarce Resources
Balancing Security & Uptime



Business critical apps
Revenue & brand reputation at risk



66% of data breaches are not discovered for months¹



Web Apps are an Easy Target

Web Applications are a favorite target for attackers¹

1

Easy to develop exploits

2

High potential value of data

78%

of initial compromises were rated as low or very low difficulty²



Top 20 Critical Controls
Application Software Security
(known initial entry point for attacks)

Top 10 Web App
Security Risks



The impact of vulnerabilities WILL be huge...

Web App Vulnerabilities

- Injection
- Broken authentication
- XSS
- Sensitive data exposure
- Cross site request forgery
- Insecure direct object references
- Security misconfiguration
- Missing Function level access control
- Unvalidated redirects

Technical Impacts

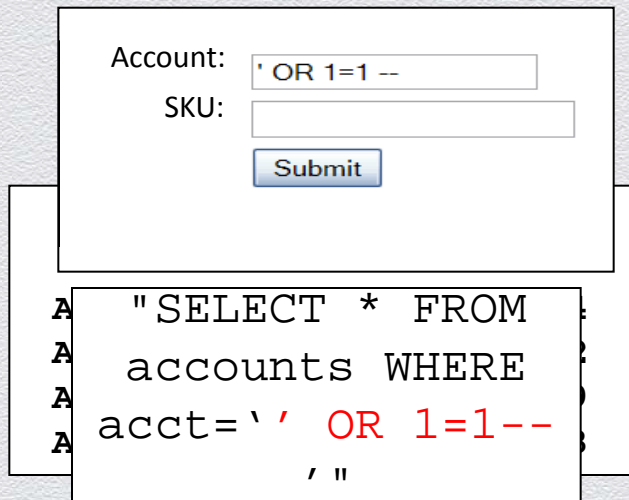
- Site defacement
- Access to databases & internal networks
- Loss of sensitive data
- Google search blacklisting
- Malware
- User accounts hijacked
- Web server downtime

Business Impacts

- Damage to brand reputation
- Loss of customer trust
- Revenue loss
- Fail PCI Compliance



#1 Most Critical Risk - Injection example



The diagram illustrates a web form and the SQL query it generates. The form has two input fields: 'Account:' and 'SKU:', with a 'Submit' button. The 'Account' field contains the text 'OR 1=1 --'. Below the form, a box shows the resulting SQL query: "SELECT * FROM accounts WHERE acct=' ' OR 1=1--', ". The 'OR 1=1 --' part of the query is highlighted in red, indicating the injected attack payload.

Account:

SKU:

```
"SELECT * FROM
accounts WHERE
acct=' ' OR 1=1--
, "
```

1. Application presents a form to the attacker
2. Attacker sends an attack in the form data
3. Application forwards attack to database in a SQL query
4. Database runs query containing attack and sends encrypted results back to app
5. Application decrypts data as normal and sends results to the attacker

Broken Authentication & Session Management

Top 10 Risk that highlights the importance of SSL certificates



www.boi.com?JSESSIONID=9FA124...

www.hacker.com



1. User logs into site with credentials
2. Site uses URL rewriting (add session ID to URL)
3. User clicks on link on page to www.hacker.com
4. Hacker checks referrer logs on www.hacker.com and finds user's JSESSIONID
5. Hacker uses JSESSIONID and takes over account on original site

Finding web app vulnerabilities



Technical Flaws

- Automated tools crawl websites, imitating user interaction to find errors in code
- Finds common coding errors like SQL injection, cross site scripting, ineffective security controls



Logical Flaws

- Looking at site in context to find potential weaknesses
- Manual testing uncovers flaws that are difficult or impossible to find with automated tools
- Proven hand testing techniques



#RSAC

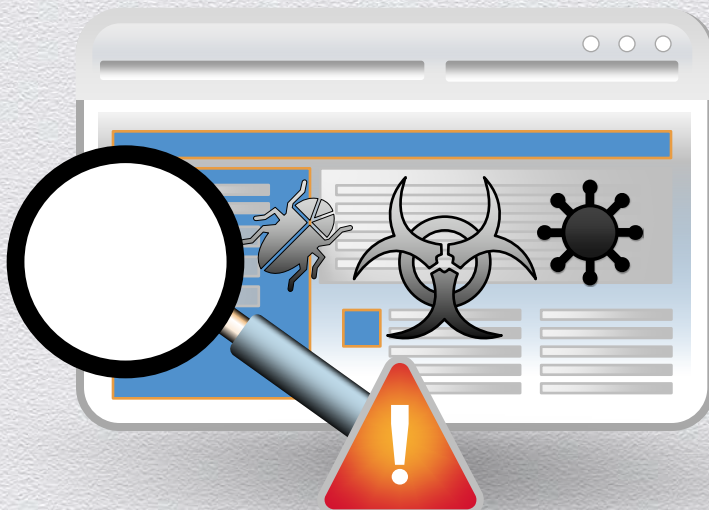
RSACONFERENCE2014

Proper Counter Measures for Securing Web Apps



DETECT

- App and Platform scanning
- Web reputation monitoring
- Malware scanning
- Hands on application logic testing



PROTECT

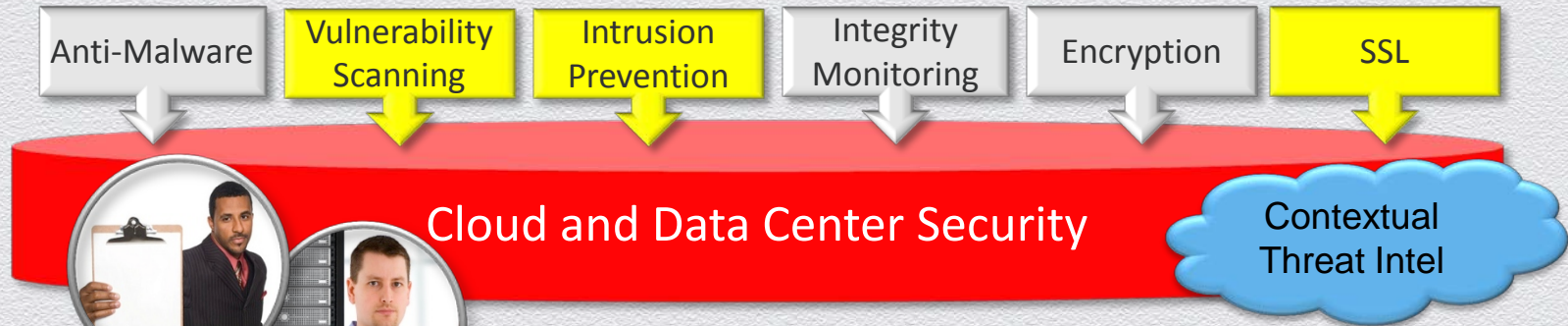
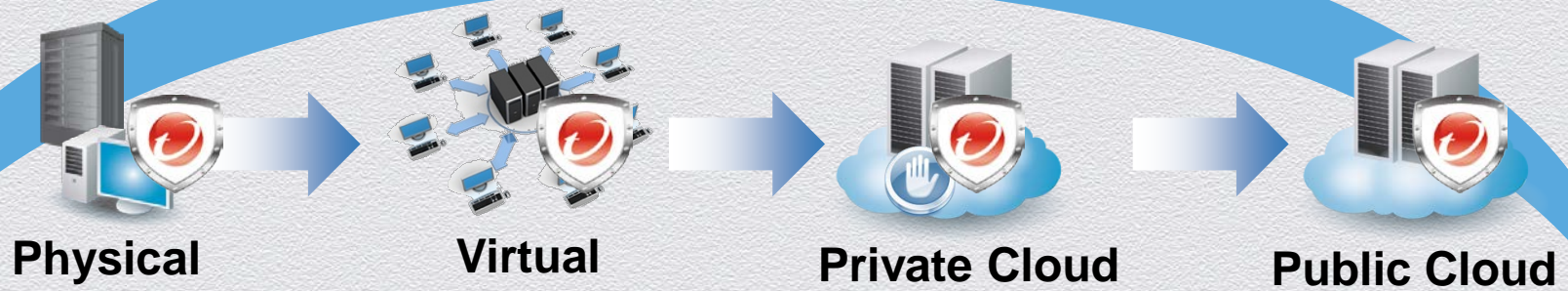
- WAF rule generation
- Intrusion prevention
- SSL certificates



#RSAC

RSACONFERENCE2014

Apps Span Ecosystems...



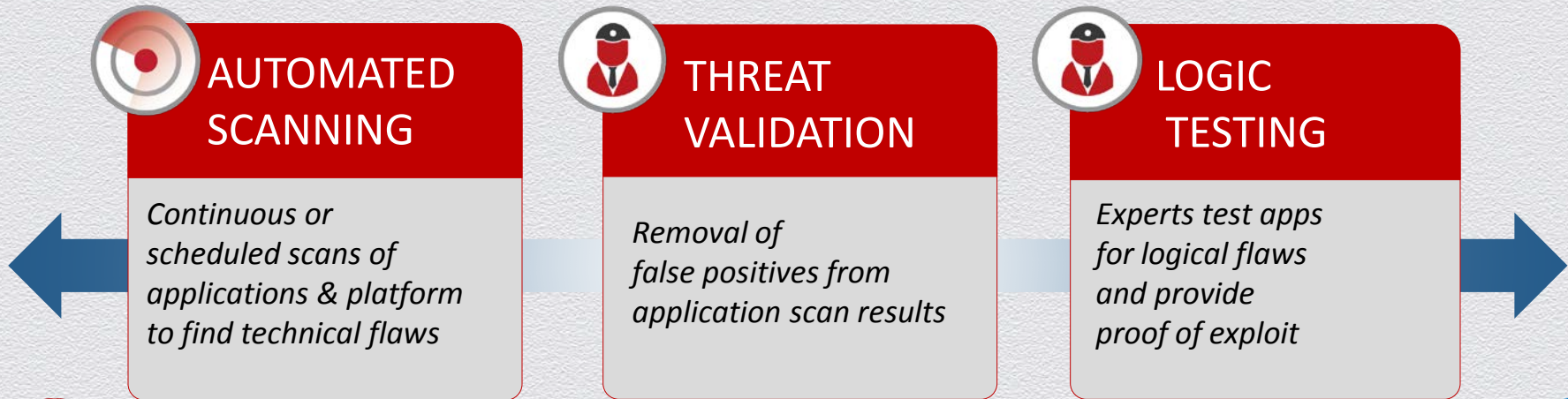
Security Ops
Data Center Ops

RSACONFERENCE2014

DETECTION

Comprehensive, Intelligent Vulnerability Testing

In-depth evaluation for testing criteria from OWASP, PCI and WASC



DETECTION

Automated Malware Detection

- ◆ Simulated user interaction discovers hidden malware
- ◆ “Neighborhood” checking for higher risk awareness
- ◆ Backed by massive threat intel

The screenshot displays the Trend Micro Malware Detection interface. The main window shows a list of scan results (84) with various categories like 'Malware Found in the Web Application', 'Malicious Page Found in the Web Application', 'Malware Found on a Foreign Link', 'Malicious Foreign Link Found', 'External JavaScript Found in the Web Application', and 'Hidden Frame Found in the Web Application'. A detailed view of a specific alert is shown in the foreground.

Malware Found in the Web Application

Severity : Critical

Description :
The web application <http://was-demo.trendmicro.com> is malware infected with JS_EXPLOIT.SM.

Details			
Alert ID	13081	Found Date	15-May-2013
Open Status	Open	First Found	11-May-2013
Verified Status	Verified		
Affected URL	http://was-demo.trendmicro.com/userinfo.htm		
Parent URL	http://was-demo.trendmicro.com/		
Malware Name	JS_EXPLOIT.SM		

DETECTION

Web Reputation Management

- ◆ Deploy a solution that checks ALL links on your site including foreign links for safety and content
- ◆ Platform should highlight potential dangers that could lead to being blacklisted by Google or blocked by browsers



The screenshot displays the 'Web Reputation' interface for the URL 'http://was-demo.trendmicro.com'. It includes sections for 'Primary Site Details' (Safety Rating: Safe), 'Foreign Link Details' (a table of links with their safety ratings), and 'Content Categorization' (General: Computers / Internet). An overlay provides a legend for the icons used in the 'Foreign Link Details' table.

Foreign Link Details	
Foreign Links	Safety Rating
hiderefer.com	Dangerous
www.faloge.com	Dangerous
bandofbros.us	Dangerous
www.owasp.org	Safe
blogs.securiteam.com	Safe
www.acunetix.com	Safe
hackers.org	Safe

The key below explains each icon used for reporting web reputation.

1. Safety Rating

- Safe** (Green checkmark): The latest tests indicate that this URL contains no malicious software and shows no signs of fraud.
- Dangerous** (Red X): The latest tests indicate that this URL contains malicious software or could defraud visitors.
- Suspicious** (Yellow exclamation mark): This URL has been compromised before, or has some association with spam email messages.
- Untested** (Blue question mark): Because you were curious about this URL, Trend Micro will now check it for the first time. Thanks for mentioning it!

2. Content Categorization

- 18+** (Red circle with 18+): **Adult** - Websites generally considered inappropriate for children.
- Business** (Green circle with dollar sign): Websites related to business, employment, or commerce.
- Network Bandwidth** (Icon of two computers): Websites offering services that can significantly impact the speed of the computer's Internet connection.
- Lifestyle** (Icon of a person): Websites about religious, political, or sexual preferences, as well as recreation and entertainment.

PROTECTION

Intrusion Prevention

- Leverage virtual patching to shield against known and zero-day platform vulnerabilities
 - no code push and/or configuration fixes
- Should include coverage for all major web servers and OS

The screenshot displays the Trend Micro Platform Protection console. On the left, a sidebar shows navigation options: Certificates, Platform Protection (selected), and Application Firewall. The main area is titled 'Platform Protection' and shows configuration for a web application at 'http://was-demo.trendmicro.coi' on server 'shiva-demo-scn1'. The 'Security Agent Status' is 'Enabled' and 'Rule Auto-deploy Status' is 'Disabled'. Below this, a table lists vulnerabilities with columns for Alert ID, Vulnerability Type, Rule Type, Status, and Last Change.

Alert ID	Vulnerability Type	Rule Type	Status	Last Change
1578	HTTP TRACE / TRACK Methods Allowed	Auto Protect	Action Required	
1925	Apache mod_negotiation Multi-Line Filename Upload Vulnerabilities	Auto Protect	Deployed	09-Oct-2013
1887	PHP 5.3.x < 5.3.26 Multiple Vulnerabilities	Auto Protect	Deployed	25-Nov-2013
1531	PHP ip2long Function String Validation Weakness	Auto Protect	Action Required	
1552	Apache Mixed Platform AddType Directive Information Disclosure	Auto Protect	Action Required	
1554				
1881				
1876				
1894				
1929				
6210				
1923				

A modal window titled 'Platform Protection Rule Information' is open, showing details for the rule 'PHP 5.3.x < 5.3.26 Multiple Vulnerabilities'. It includes a table with CVE-ID, Rule Name, Application Type, and Description.

CVE-ID	Rule Name	Application Type	Description
CVE-2013-2110	PHP Heap Based Buffer Overflow Vulnerability	Web Application PHP Based	Heap-based buffer overflow in the quoted_printable_encode function in PHP allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted argument.

A 'BACK' button is visible at the bottom of the modal.



- Adding an SSL layer to your web applications furthers defense in depth
- Obtain from a globally trusted Certificate Authority
- Certificates must be supported in all of the major browsers
- Acquire a platform that is highly scalable and has a simplified management console to meet the needs of the largest organizations

Web App Security Platform DNA

- 1 Comprehensive Detection: Continuous, automated scanning of applications and platforms, plus app logic testing by security experts
- 2 Automated Protection: Virtual patching of discovered platform vulnerabilities and WAF rule generation
- 3 Strategy should consist of best of breed proprietary tools as well as open source capabilities
- 4 Policy, Training and build into requirements/design phase of SDLC



RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO



Thanks for your time!
@jdsherry
jd_sherry@trendmicro.com