United States Army
Criminal Investigation Command

Media contact:
571-305-4041

FOR IMMEDIATE RELEASE

Hunting The Hackers

CCIU Detectives Deliver Digital Justice

By Colby Hauser
CID Public Affairs

QUANTICO, VA, Jan 7, 2013 — No other environment within the modern era has evolved as rapidly and as exponentially as the Internet. Traversing this virtual jungle, a global community of users takes advantage of almost unlimited access to news, information and services by the simple click of a mouse or a tap on a Smartphone. In today's digital age time waits for no one, unfortunately neither does crime.

Throughout the world legions of cyber predators' hunt, stalk, plot, and attack unsuspecting systems, networks and users in an effort to advance their criminal enterprise. And yet another apex predator inhabits this world, the U.S. Army CID's Computer Crimes Investigative Unit (CCIU), turning the tables on those would-be predators to where the hunters now have become the hunted.

"CCIU is the U.S. Army's sole entity for conducting worldwide criminal investigations of computer intrusions and related national security threats affecting U.S. Army computers, networks, data and personnel," said Special Agent Daniel Andrews, the director of CCIU. "Intruders range from non-malicious hackers to those intent upon disrupting a network or website, to foreign intelligence probes, so that makes our mission extremely important not just for CID, but the United States Army."

"Dependency on computer technology has saturated almost every aspect of our lives, both within the Army and the civilian world, so the opportunity for cyber crime will only continue to increase," he added.

Just up the road from the FBI National Academy on Marine Corpes Base Quantico, Virginia, and within the labyrinth of the Defense Department's Russell-Knox Building,

-more-

lays the command and control of the Army's digital detectives. As the sole entity for conducting criminal investigations involving Army computer networks, CCIU maintains a constant watch and a continuous presence over the Army's digital footprint.

"Our investigations have led to arrests of Soldiers, civilians and foreign nationals throughout the world who were engaged in cybercrime directed at the U.S. Army," Andrews said. "Regardless of where a crime is committed or the judicial venue in which it's prosecuted, if you commit a crime against the Army, we will find you and bring you to justice."

With personnel assigned to subordinate field elements at various domestic and overseas locations, the special agents, attorneys and information technology professionals of CCIU are tasked with a very challenging and growing mission.

Army CID recognized the expanding role of computers in criminal activities and investigations, and provisionally established CCIU as the Computer Crime Investigative Team in January of 1998. Prior to this, only a single forensic examiner at the U.S. Army Criminal Investigation Laboratory (USACIL), was dedicated to investigating computer crime.

Andrews explained that the CCIU was originally created out of the Field Investigative Unit (FIU), a specialized unit within CID that investigates classified and special access programs, and given the primary responsibility for investigating intrusions into U.S. Army computer networks.

"In November of 1999 we separated from FIU, becoming a subordinate element of the 701st Military Police Group (CID)," Andrews said.

In January 2000, CCIU was officially established as a criminal investigative unit within CID.

Because investigations of this nature require a specialized level of computer expertise, CCIU is comprised of civilian Special Agents, many of whom served in uniform as CID Special Agents, before specializing in computer crimes and cyber security.

"There is always a digital evidence component to every investigation we do," said Special Agent Edward Labarge, a former Marine CID special agent, now an agent with CCIU. "That number has increased significantly over the last couple of years as advances in both hardware and software are exploited and employed by those people who would target the Army."

This fact has greatly impacted conventional CID investigations as well. Answering this call, training opportunities exist for active duty CID special agents, such as the Digital Forensic Examiner (DFE) program that serves as an outstanding bridge to becoming a CCIU special agent. The program covers a myriad of different tactics and techniques specific to processing digital evidence for law enforcement purposes.

Labarge said although all CCIU special agents are qualified to serve as a DFE, that mission is primarily performed by CCIU's Digital Forensic Research Branch (DFRB).

"When we execute a warrant, we routinely collect lots of digital evidence such as hard drives, digital images of servers, but we turn that over to the DFRB so we can focus on the actual criminal investigation," he said.

Agents assigned to CCIU receive advanced computer training from the Defense Cyber Investigations Training Academy, the Federal Law Enforcement Training Center and from other technical experts. CCIU Special Agents also use their specialized knowledge of information technology to provide guidance to other CID Special Agents who conduct investigations involving computers and other electronic media.

Since its creation, CCIU has been a key element in the successful prosecution of numerous computer intrusion matters and has been recognized around the globe. A recent example of the far-reaching digital arm of CCIU involved a suspected Romanian hacker who attempted to illegally gain access to both the U.S. Army and NASA computer networks.

Andrews explained that although CCIU was unsuccessful in getting the case prosecuted in the U.S., CCIU continued to press on with the investigation and joined forces with their international law enforcement partners.

"Not only did we stop this individual from gaining access, but we were able to successfully prosecute him in Romania," he said. "Just because a person commits the crime overseas doesn't mean that our investigation stops or that justice won't be carried out. We simply adapt to ensure that in the end, justice is served."

With quite an impressive track record, CCIU, as well as Special Agents and alumni, have been honored for their expertise and development of technological products in the realm of cyber security.

"CCIU is one of the best outfits working in cyber law enforcement today," said Howard Schmidt, a former Special Assistant to the President of the United States and Cyber Security Coordinator. Schmidt, a retired CID Special Agent, was appointed by President Obama to head cyber security for the White House while serving at CCIU.

"Without my time in CID and government service, I don't know if I would have had the insight and depth of understanding of government and how it relates to cyber security," Schmidt said. "I think that staying involved in those communities helped tremendously."

Regarding technological products developed at CCIU, the Rapid Extraction and Analysis Program or REAP software has been worth its weight in gold. Time, manpower and a global mission, often prevents agents from physically responding to every cyber incident and CCIU needed a solution to help. The REAP program was that solution.

"The REAP program allows our agents to conduct a virtual autopsy on hacked systems and extract digital evidence so we can track down those responsible and bring them to

justice," Andrews said. "This allows our special agents to adapt to any given situation during the course of an investigation."

The program was developed in-house, at no cost to the government, and allowed non-CCIU personnel to deploy the program across various Army computer platforms. Once deployed, the program preserves collected digital evidence in an automated manner following computer intrusions, expedites critical threat information to network defenders, and analyzes malicious software.

Currently, the REAP program is deployed with the Army's Computer Emergency Response Team (ACERT) and all of the Regional Computer Emergency Response Teams (RCERT).

Andrews said as a testament to REAP's effectiveness, the interagency Technical Support Working Group has funded the program for further development as Government Off-The-Shelf software that can be freely shared with any federal agency.

Looking towards the future, CCIU continues to do what has to be done, and encourages their fellow special agents to be mindful of the digital battleground.

"As the Army continues to move forward by incorporating technology into all aspects of operations, they will become a target of opportunity for cyber criminals," Andrews said. "But we will be here to stop them, dead in their tracks."

For more information on Army CID visit www.cid.army.mil

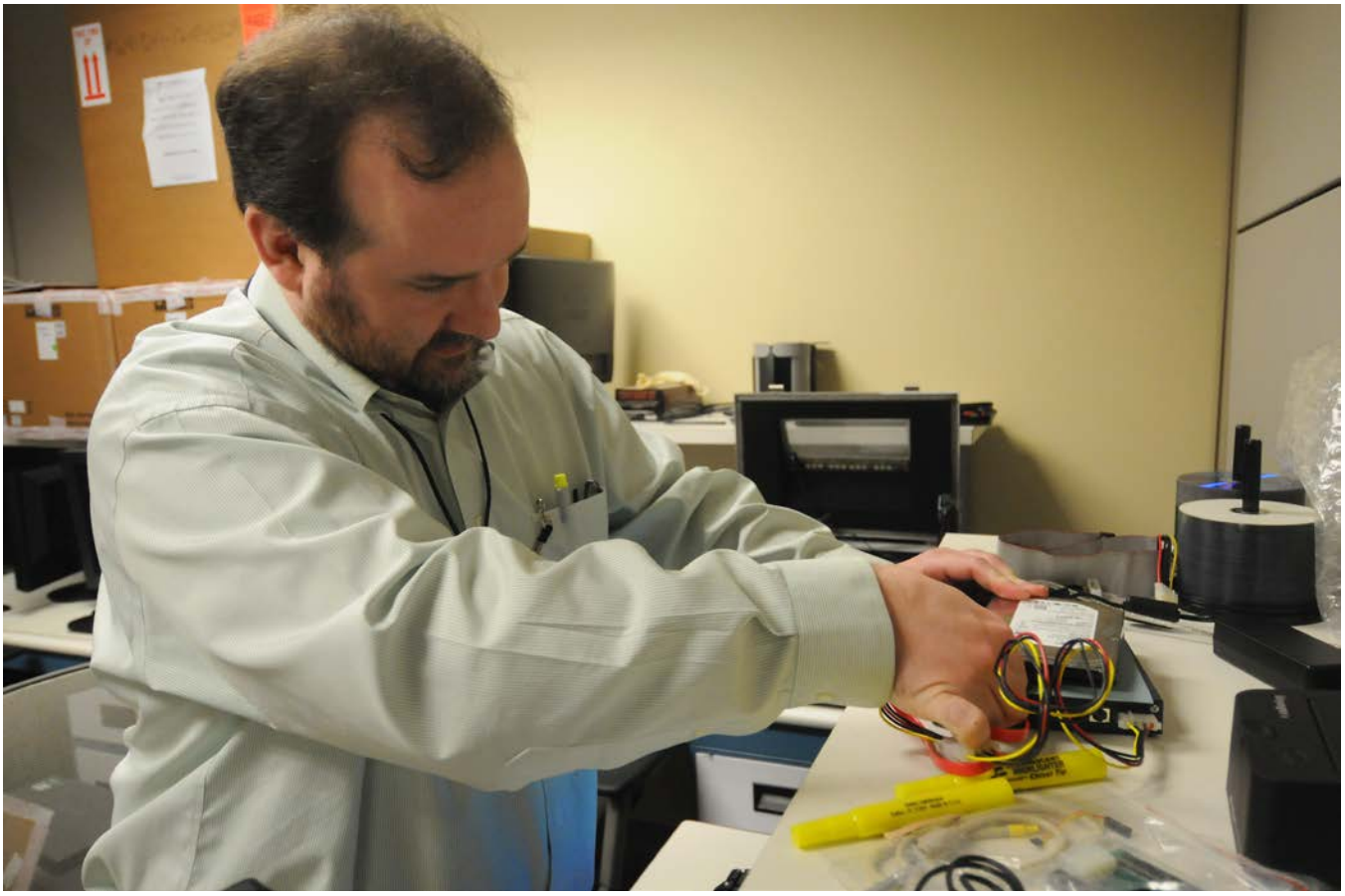
-30-

Embedded Photos attached

5-5-5 CCIU

Special Agent Edward Labarge, an agent with the Computer Crimes Investigative Unit (CCIU) at Quantico, VA, conducts investigative research into a suspected network populated by computer hackers' intent on illegally accessing a restricted Army network. (U.S. Army photo by Colby T. Hauser, CID PAO)

6-6-6 CCIU



Mr. Mark Johnson, a digital forensic examiner with the Computer Crimes Investigative Unit (CCIU) at Quantico, VA, pulls digital information off of a confiscated hard drive for further examination. (U.S. Army photo by Colby T. Hauser, CID PAO)

For more information on Army CID visit www.cid.army.mil

-30-